12-09-99 A

UTILITY PATENT APPLICATION TRANSMITTAL
(Only for new nonprovisional applications under 37 CFR 1.53(b))

Docket No.	:	34581/CAG/C718
Inventor(s)	:	Jay C. Chen
Title	:	A CRYPTOGRAPHIC SYSTEM AND METHOD FOR ELECTRONIC TRANSACTIONS
Express Mail Label No.	:	EL368761445US

ADDRESS TO: Assistant Commissioner for Patents
Box Patent Application
Washington, D.C. 20231

Date: December 8, 1999

1. _X_ **FEE TRANSMITTAL FORM** *(Submit an original, and a duplicate for fee processing).*

2. **IF A CONTINUING APPLICATION**

____ This application is a of patent application No. .

_X_ This application claims priority pursuant to 35 U.S.C. §119(e) and 37 CFR §1.78(a)(4), to International Application No. PCT/US99/09938, filed May 5, 1999, which claims priority of U.S. Provisional Application No. 60/084,257, filed May 5, 1998.

3. **APPLICATION COMPRISED OF**

Specification

_55_ Specification, claims and Abstract (total pages)

Drawings

_29_ Sheets of drawing(s) (FIGS. 1 to 13)

Declaration and Power of Attorney

___ Newly executed
_X_ No executed declaration
___ Copy from a prior application (37 CFR 1.63(d))(for continuation and divisional)

4. ____ **Microfiche Computer Program** *(Appendix)*

5. ____ **Nucleotide and/or Amino Acid Sequence Submission** *(if applicable, all necessary)*

___ Computer Readable Copy
___ Paper Copy (identical to computer copy)
___ Statement verifying identity of above copies

6. **ALSO ENCLOSED ARE**

____ Preliminary Amendment
____ A Petition for Extension of Time for the parent application and the required fee are enclosed as separate papers
____ Small Entity Statement(s)
___ Statement filed in parent application, status still proper and desired
___ Copy of Statement filed in provisional application, status still proper and desired

UTILITY PATENT APPLICATION TRANSMITTAL
(Only for new nonprovisional applications under 37 CFR 1.53(b))

Docket No.: 34581/CAG/C718

____ An Assignment of the invention with the Recordation Cover Sheet and the recordation fee are enclosed as separate papers

____ This application is owned by pursuant to an Assignment recorded at Reel , Frame

_X_ Information Disclosure Statement (IDS)/PTO-1449

_X_ Copies of IDS Citations

____ Certified copy of Priority Document(s) *(if foreign priority is claimed)*

____ English Translation Document *(if applicable)*

_X_ Return Receipt Postcard (MPEP 503) (should be specifically itemized).

_X_ Other: Petition to Make Special and Filing fee of $130.00 for the Petition to Make Special

7. CORRESPONDENCE ADDRESS

CHRISTIE, PARKER & HALE, LLP, P.O. BOX 7068, PASADENA, CA 91109-7068

Respectfully submitted,

CHRISTIE, PARKER & HALE, LLP

By Craig A. Gelfound

Craig A. Gelfound
Reg. No. 41,032
626/795-9900

CAG/cmm

A CRYPTOGRAPHIC SYSTEM AND METHOD FOR ELECTRONIC TRANSACTIONS

CROSS-REFRENCE TO RELATED APPLICATIONS

The present application claims priority of PCT Application Entitled A CRYPTOGRAPHIC SYSTEM AND METHOD FOR ELECTRONIC TRANSACTIONS, International Application No. PCT/US99/09938, filed May 5, 1999, which claims priority of U.S. Provisional Application No. 60/084,257 filed on May 5, 1998.

FIELD OF THE INVENTION

The present invention relates generally to a cryptographic system and method for secure electronic transactions, and more particularly to an electronic card, which takes the form of a "smart card" and/or its equivalent software.

BACKGROUND OF THE INVENTION

The generic term, "smart card," generally denotes an integrated circuit (IC) card, that is, a credit-card-size piece of plastic with an embedded microchip. The IC chip on a smart card generally, but not necessarily, consists of a microprocessor (the CPU), read-only memory (ROM), random access memory (RAM), an input/output unit, and some persistent memory such as electrically erasable programmable read-only memory (EEPROM). The chip can perform arithmetic computations, logic processing, data management, and data communication.

Smart cards are mainly of two types: contact and contact-less. The International Standard Organization (ISO) has established specifications for such electronic cards under the ISO series. In particular, ISO 7816 applies to integrated circuit(s) cards. Because of its computing capability, a smart card can support a multitude of security features such as authentication, secured read/write, symmetric key and asymmetric key encryption/decryption. These smart card security features make it well suited for electronic commerce where data security and authenticity are of primary importance.

Smart card use has found application in many specialized fields such as mass transportation, health insurance, parking, campus, gas, etc. And its potential use in electronic commerce and other financial areas are gaining popularity at a rapid pace. U.S. Pat. No. 5,521,362, issued to Robert S. Power on May 28,1996, entitled "Electronic purse card having multiple storage memories to prevent fraudulent usage and method therefore,"describes an electronic purse application. Power's invention demonstrates a smart card's capability to be used as a secure financial instrument and not just as a storage device.

As advances in technology push smart-card chip computing to higher speeds and larger memory capacity, the concept of a "multi-application" smart card is increasingly becoming economically and physically feasible. U.S. Pat. No. 5,530,232 issued to Douglas C. Taylor on June 25, 1996, entitled "Multi-application data card," describes a multi-application card, which is capable of substituting for a plurality of existing single-application cards and satisfying both financial and non-financial requirements. The multi-application card uses a conventional data link to connect between the smart card and the remote service provider. Taylor's invention, the multi-application card, does not relate to any kind of open network or cryptographic method.

U.S. Pat. No. 5,544,246 issued to Mandelhaum et al. on" on Aug. 5, 1996, entitled "Smart card adapted for a plurality of service providers and for remote installation of same," describes a smart card, which allows different service providers to coexist on the same smart card. Each service provider is considered a user of the smart card and is installed on the card by the issuer/owner of the smart card. Each user is allowed to build a tree-like file structure and protect it with a password file. Mandelbaum's invention depicts a smart card allows for the creation and deletion of multiple applications. Mandelbaum's smart card controls the access to each application by using an appropriate password file.

U.S. Pat. No. 5,671,279 issued to Taher Elgamal on September 23, 1997, entitled "Electronic commerce using a secure courier system," describes a system for implementing electronic commerce over a public network using public/private key cryptography. The Elgamal patent did not mention the use of a smart card as a tool in conducting the electronic commerce and the participants were authenticated through the use of digital certificates. The secure courier system requires a secured channel such as a Secure Socket Layer (SSL) between the trading parties over an open network such as the Internet.

U.S. Pat. No. 5,790,677, issued to Fox et al. on August 4, 1998, entitled "System and method for secure electronic commerce transactions," describes a system and method having a registration process followed by a transaction process. During the registration phase, each participant of a transaction registers with a trusted credential-binding server by sending to the server a registration packet. The server produces unique credentials based upon the request received and sends them to the request originator. During the transaction phase, the originator of the transaction requests, receives and verifies the credentials of all intended recipients of the commerce document and/or instrument and encrypts the document and/or instrument using the public key of the individual recipient. Thus, each receiving party can decrypt and access the information intended only for him. Fox's patent describes a process which reflects the theme of the so called "Secure Electronic Transaction" (SET) standard which is an ongoing effort supported by several major financial and software companies to establish a digital certificate and certificate authority based electronic commerce system.

U.S. Pat. No. 5,796,840 issued to Derek L. Davis on August 18, 1998, entitled "Apparatus and method for providing secured communication," describes a semiconductor device, which is capable of generating device-specific key pairs to be used in subsequent message authentication and data communication. The semiconductor device uses public/private key cryptography to ensure the authenticity of two communicating parties.

U.S. Pat. No. 5,534,857 issued to Simon G. Laing and Matthew P. Bowcock on July 9, 1996, entitled "Method and System for Secure, Decentralized Personalization of Smart Cards," describes a method and apparatus for securely writing confidential data from an issuer to a customer smart card at a remote location. A mutual session key for enciphering data transfer between a secure terminal and a secure computer is generated by using a common key stored in the secure computer and a retailer smart card.

It is clear from the inventions mentioned above that the architecture of a secure electronic commerce system involves a public key infrastructure and digital certificate authority associated with it.

On an open network, a secret key-based system is less flexible in terms of key distribution and key management, and is more subject to malicious attack. On the other hand, a public/private key-based system, with all its advantages over the secret key system, has its own daunting task of authenticating transaction parties to one another. The current invention presents another system and method, which replaces the need for certificate authorities and digital certificates. The current invention is a hybrid system for electronic transactions. The hybrid system uses public/private keys during the key exchange phase and uses a session key as a secret key during the transaction phase.

SUMMARY OF THE INVENTION

In one aspect of the present invention, the system for electronic transactions comprises: an electronic card having a cryptographic service for encryption and decryption, a data area for storing cardholder information, and a data area for storing service provider information; a service provider member terminal responsive to activation of the electronic card; and a service provider terminal in communication with the service provider member terminal, the service provider terminal decrypting communication from the service provider member terminal and encrypting communication to the service provider member terminal, the service provider member terminal encrypting communication to the service provider terminal and decrypting communication from the service provider terminal.

In another aspect of the invention, the method of conducting an electronic transaction using an electronic card comprises formatting a key exchange request message at a member, sending the key exchange request message from the member to a service provider, generating a session key at the service provider, formatting a key exchange response message including the session key at the service provider, sending the key exchange response message from the service provider to the member and using the session key to conduct a transaction.

In yet another aspect of the invention, the method of conducting an electronic transaction using an electronic card comprises formatting a key exchange request message at a member, the key exchange request message has a member challenge for the service provider, sending the key exchange request message from the member to a service provider, generating a session key at the service provider, formatting a key exchange response message including the session key at the service provider, the key exchange response message has a response for the member challenge and a service provider challenge for the member and sending it to the member, formatting by the member a response for the service provider challenge and sending it to the service provider and using the session key to conduct a transaction.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a block diagram showing the relationship among the components of a system according to an embodiment of the invention.

Figure 2 shows the flow of the two transaction phases via a network.

Figure 3 is the diagrammatic representation of an EC.

Figure 4 shows the format of the service provider data area. Each service provider's information is allocated an entry in the table and is protected by access conditions.

Figure 5 shows how the digital signatures are used in an embodiment of the invention.

Figures 6A through 6Q shows the schematic flow chart of the cryptographic system and method used in an embodiment of the invention in order to conduct electronic transactions via an open telecommunication network, such as the Internet.

Figure 7 through Figure 11 depicts the final format and content of the combined request and response messages in the key exchange phase and the transaction phase.

Figure 12 shows a service provider conducting a transaction with participants that have been arranged in series.

Figure 13 shows a service provider transaction on a network with participants that have been arranged in a hierarchical organization scheme.

DETAILED DESCRIPTION

A preferred embodiment of the invention is a cryptographic system and method for electronic transactions by using an electronic card (EC) in the form of a smart card or equivalent software and communicating over a communications network.

The preferred embodiment of the invention uses an open network, such as the Internet.

Alternative embodiments of the invention may use other types of networks. An embodiment of the invention may either use a physical smart card, or alternatively, a smart card, which is implemented as computer software package and runs on a computing device such as a personal computer (PC). Likewise, a merchant involved in a transaction may use a merchant device, which is a point-of-sale terminal, or a device, which uses software on a host computer to communicate with an EC and a service provider. When a smart card is used, a smart card reader is also needed to allow the card to communicate with a host device, such as a network ready merchant terminal, a PC, or any other electronic device, which is capable of supporting smart card transactions.

In a public key and digital certificate based system, transaction participants exchange public information through the use of digital certificates or other electronic credentials which are issued and certified by a certificate authority (CA) or credential binding server. The communication between the CA or the server and each participant of the transaction must be secure. Random numbers and digital signatures are used to ensure the authenticity and validity of the messages transmitted among the participants.

The cryptographic system and method of the preferred embodiment of the invention also uses public/private key cryptography, but it works in a slightly different way. The cryptographic system and method does not seek to create another kind of trust relationship as the one that exists between holders of digital certificates and the certificate authorities. It particularly targets large membership-based financial institutions such as a large credit card company and all its cardholders, or a major bank and all its ATM cardholders as its potential users. Non-financial institution can also use this cryptographic system and method to conduct commercial or non-financial transactions over a network.

A service provider (SP) provides some service to its members. Financial institutions are just one kind of service provider. A service provider can also be non-financial in nature. Regardless whether a service provider is a financial institution or a non-financial institution, essentially the same process occurs. The only difference between a transaction involving a financial institution and a transaction involving a non-financial institution is that the messages may include different data fields.

When an EC holder signs up with one of the service providers, the service provider creates a dedicated entry on the EC. Each entry contains the account information for the service provider, the SP's public key, access control information, and other related data. Each EC can support a predetermined number (e.g. ten) of such entries and each such entry is a representation of one service provider.

By using the public/private key cryptography, the key distribution process is much simplified. The EC holder him/her/self or any trusted third party such as a bank branch or even a post office can perform the task. The SP's public key is only used for the initial key exchange between the SP and the cardholder. After the initial key exchange step, the SP assigns a session key, which protects any further message exchange between the cardholder and the SP or between the cardholders' themselves.

This hybrid system, which uses both public key/private key cryptography and secret key cryptography (i.e., session key), is in contrast to other secret-key systems in that in the hybrid system, the secret key (i.e., session key) is valid for a single session and is not applicable to other sessions. A session has a determinate length of time. A session may terminate based upon a time period or upon conditions being satisfied.

Where a merchant is involved in a transaction, the merchant goes through essentially the same procedures as the EC holder to communicate with the SP. The merchant will first perform a key exchange with the SP and receive a session key. The session key will be used by the merchant for subsequent communication with the SP. The cardholder and the merchant digitally sign each message going to the SP and the SP similarly signs the response message going back to the cardholder and the merchant.

In the event that a transaction requires interactions with another certificate-based system, the SP, after authenticating the cardholder and the merchant based on further information exchange after the initial key exchange, can act as a surrogate-certificate for the cardholder and the merchant. In the most extreme case, the SP performs solely this surrogate function and becomes a gateway for the certificate-based system. This type of hierarchy is highly desirable since it reduces the number of trust relationships needed to carry out a transaction among multiple systems. In addition, it eliminates the users' need to carry certificates.

The preferred embodiment of the invention is a cryptographic system and method for electronic transactions by using an electronic card (EC) in the form of a smart card or equivalent software and communicating over a communications network.

In the preferred embodiment of the invention, the network is an open network such as the Internet. In alternative embodiments of the invention, other open networks and/or closed networks may be used to establish communication between a service provider and its members. For example, a service provider may use its own proprietary financial network to communicate with its members.

Any Internet protocol may be used for Internet connections. Example protocols, which can be used include TCP/IP, UDP, HTTP, and the like.

Communication may also be via a communications network transport service such as the Public Switched Telephone Network (PSTN) using traditional analog telephone service (a.k.a. Plain Old Telephone Service or POTS), or by using a digital communication service such as a T-1, E1 or DS-3 data circuit, Integrated Services Digital Network (ISDN), Digital SubscriberLine (DSL) services, or even using a wireless service, and the like. When implemented using such a service the invention may be implemented independent of a communications protocol (i.e. at an electrical interface layer).

Communication may also be via a local area network (LAN) or Wide Area Network (WAN) such as Ethernet, Token Ring, FDDI, ATM or the like. Example protocols, which can be used include TCP/IP, IPX, OSI, and the like.

Other communication links might include an optical connection, a wireless RF modem connection, a cellular modem connection, a satellite connection, etc.

The invention may be employed as long as a communication path can be established between a service provider and its members. The examples above are intended to illustrate several examples of the various communications environments in which the invention may be practiced. As is clear to one ordinarily skilled in the art, the invention is not limited to those environments detailed above.

The EC can take the form of a smart card device or a software package running on a computer system such as a personal computer (PC). When the EC is implemented on a smart card, it can be used on a network-ready computer system such as a PC to transact with another member and/or a selected service provider. It will need a read/write interface device to communicate with a computer system and some application software such as an Internet browser to interface with the cardholder and the network. If the EC is a software package loaded into a computer system, then no read/write interface is needed. The exemplary embodiment of the invention is for the EC to act as an electronic wallet (or cyber wallet) which functions similar to real wallet. A real wallet can carry credit cards, debit cards, ATM cards, health provider cards, membership cards, cash, etc. An EC has the digital equivalent of all the above-mentioned financial and non-financial instruments and enables conducting secure transactions over the Internet.

A service provider member can be a merchant and/or an EC cardholder. A merchant is a member who is paid by the service provider as a result of a transaction. A member can be both a merchant and an EC cardholder. A merchant may engage in a transaction with other cardholders, which results in the merchant being paid by the service provider. A merchant may also be an EC cardholder and purchase supplies, for example, from a merchant supplier.

The cryptographic system may involve communication between a service provider and any number of service provider members. Thus, communication can be between an EC and an SP, between a merchant and an SP, between a first EC, a second EC, and an SP, between a first merchant, a second merchant, and an SP, etc. An EC may communicate directly with a service provider to inquire about an account balance for example. A merchant may communicate with a service provider only on his own behalf and not on behalf of an EC because, for example, the merchant wants to know his own account balance with the service provider. Communication between the SP and its members may follow any permutation of the SP and its members. The organization of the communication links between the SP and its members may be serial and/or hierarchical. Communication between the SP and its members may also be serial and/or via routers, which route the messages between the SP and its members.

The cryptographic method is a two-phased key-exchange-transaction model. The first phase is a key exchange phase. The second phase is the transaction phase. In the key exchange phase, the members exchange keys with the service provider. The members send their keys to the service provider and the service provider uses the keys to send a session key to the members. The session key protects any further message exchange between the cardholder and the SP or between the cardholders' themselves. In the transaction phase, either the SP can direct the transaction or the cardholders themselves may conduct the transaction.

Figure 1 is a block diagram showing the relationship among the components of a system according to an exemplary embodiment of the invention involving a cardholder, a merchant, and service provider.

An EC cardholder 20 can conduct a transaction over a network 50 and communicate with a merchant either by using an EC read/write device 82 attached to an originating computer 84 or by using EC equivalent software 92 running on an originating computer unit 90.

A merchant can conduct a transaction over a network by either using a network-ready point-of-sale(s) (POS) terminal 40 or by using EC equivalent software running on a merchant device 70 to conduct an electronic transaction with a selected service provider 60 via a network 50 such as the Internet.

Once the access conditions to the card have been satisfied, the cardholder can perform financial or non-financial transactions with other participants of the system through the network 50. In Figure 1, there are three different scenarios in which a transaction over a network can be conducted.

(1) In a POS transaction (Upper left side of figure 1), the cardholder 20 swipes/inserts an EC through/into a merchant's EC reader/writer 30 at a merchant's premises. The EC reader/writer is connected to a network-ready merchant POS terminal 40. The network-ready merchant POS terminal 40 is a secure tamper-resistant programmable device comprising an input means such as a keyboard, a display device, a processing unit, and an EC read/write device 30 (an EC interface device). It is typically a small computer unit such as a PC equipped with a communication link to an open network.

The POS terminal communicates to the SP via the network 50.

(2) (Right side of figure 1) A cardholder can conduct a transaction with other participants of the system by inserting the EC 20 into a read/write device 82, which is connected to the cardholder's personal computer 84 which is the originating computer. The originating computer connects to a network 50 allowing the EC to communicate with the merchant computer unit 70. The merchant computer unit 70 has EC equivalent software 72 that enables the merchant to receive the EC generated message and generates a message combining EC information and merchant information. Then, the combined message is sent to the SP over a network.

(3) (Bottom side of figure 1) A cardholder can conduct a transaction with other participants of the system by using EC equivalent software 92 on the customer cardholder's personal computer 90. The transaction begins at the originating computer unit 90, that is, the cardholder's personal computer. The cardholder conducts the transaction over a network 50 and communicates with the merchant's computer unit 70, which in turn communicates with the SP 60 over a network 50.

While in the preferred embodiment of the invention, a personal computer is used to hold the EC equivalent software, in alternative embodiments of the invention other electronic devices can be used to hold the EC equivalent software.

In the preferred embodiment of the invention, the network used to enable the EC to communicate with the merchant is the same network used to enable the merchant to communicate with the SP. In another embodiment, the network used to enable the EC to communicate with the merchant may not be the same network used to enable the merchant to communicate with the SP. In yet another embodiment, the network used to enable one merchant to communicate with the SP may not be the same as the network used to enable another merchant to communicate with the SP. In still yet another embodiment, the network used to enable an EC to communicate to the merchant may not be the same as the network used to enable another EC to communicate with another merchant. An embodiment may consist of a multiplicity of networks whereby different parties communicate.

In the preferred embodiment of the invention, a transaction is broken down into two phases: a key exchange phase and a transaction phase. Figure 2 is a specific case, which illustrates the two-phase key-exchange-transaction model where the SP directs the transaction phase. There is no direct exchange of sensitive information between participants when the SP directs the transaction.

The key exchange phase is the same where the transaction phase is among the cardholders themselves and where the SP directs the transaction phase. Where the transaction phase is among the cardholders themselves, the cardholders use the SP session key to communicate with each other and conduct a transaction.

Figure 2 demonstrates a financial transaction where the SP directs the transaction phase. The transaction shown involves three parties: an EC (a transaction originator) 102, a merchant 104, and a service provider (SP) 106. The originating party is an EC cardholder who is the consumer and is represented by the computer unit 102. The computer unit 104 represents the merchant. The computer unit 106 represents the service provider. An SP is selected by both an EC and merchant.

Figure 2 demonstrates a financial transaction wherein the process flow is from an EC to a merchant to an SP. The cryptographic method's process flow is not limited to any particular order between merchants and EC cardholders. Figure 2 is merely an example of a particular transaction, which flows from EC to merchant to service provider. The process flow can also go from merchant to EC to service provider. Figure 2 demonstrates how service provider members (in this case, the EC cardholder and the merchant) create, append, and send messages to a service provider.

The ten arrows numbered 1 to 10 in figure 2 show how the messages flow among the three parties during the two transactions phases. Steps 1 through 4 belong to the key exchange phase and steps 5 through 10 belong to the transaction phase. In figure 2, the merchant serves as an intermediary between the EC and SP. In step 1, the key exchange request is formatted by the EC and sent to merchant. In step 2, the merchant combines his own key exchange message with the EC's key exchange message and sends the combination key exchange message to an SP. In step 3, the SP formats a key exchange response for the merchant, formats a key exchange response for the EC, combines the key exchange responses to form a combined key exchange response and sends the combined key exchange response to the merchant. In step 4, the merchant separates the key exchange response for the merchant from the key exchange response for the EC and forwards the EC's key exchange response message back to the EC. Step 4 concludes the main activities in the key exchange phase.

The transaction phase begins with step 5. In step 5, the EC formats its transaction request message and sends it to merchant. In step 6, the merchant combines the received transaction request message with his own transaction request message and sends the combination transaction request message to the SP. In step 7, the SP formats a transaction response message for the merchant, formats a transaction response message for the EC, combines the transaction response messages and sends the combined transaction response message back to merchant. In step 8, the merchant separates the transaction response message for the merchant from the transaction response message for the EC and forwards the EC's transaction response message back to the EC. In step 9, the EC formats a confirmation message and sends it to the merchant. In step 10, the merchant combines the received confirmation message with his own confirmation message and sends the combination confirmation message the SP. Step 10 concludes the transaction phase of a transaction.

While figure 2 demonstrates a simple transaction, some transactions may involve multiple messages. During some transactions, more than one message may be required to complete each phase, in which case, those messages will follow the same rules of combination and flow pattern. For example, during the transaction phase, the SP may require that the EC and the merchant send over account information first. If the account information is verified to be valid, the SP sends confirmation of the account information in the response message. Once the merchant and the EC receives the response message, then the EC and the merchant send the transaction amount and other transaction related information in the next message going to the SP. The SP subsequently approves or disapproves the transaction. The steps in figure 2 apply to both the account message and the transaction message.

If the completion of a transaction requires interaction with some external system such as a public key and digital certificate based system 108, the SP will act as a surrogate-certificate for the EC and the merchant and deal with the external system on behalf of the EC and the merchant. A desired result of the invention is to shield all of the participants of a transaction from an external system and therefore reduce the number of trust relationships needed to complete a transaction. If a participant of a transaction has dual membership of this system and an external system, then he has a choice of either acting as a member of this system or as a member of an external system. In the latter case, the SP will interface with the participants using the rules of an external system. For example, to deal with an external public and digital certificate or credential based system, the SP has in its possession all of the required certificate(s) or credential(s) which satisfies the trust relationship demanded by the external system. Such credentials are required in order for the SP and the external system to complete the transaction initiated by the EC and the merchant. In this case, only the SP needs to have a trust relationship with the external system. Based on this trust relationship, individual ECs and merchants are able to complete transactions with the hypothetical external system.

Figure 3 is a diagrammatic representation of a preferred embodiment of an EC. In a preferred embodiment of the invention, an EC is internally composed of the software/hardware components shown in Figure 3. The EC is ISO 7816-based and supports the same kind of communication protocols and commands as defined in ISO 7816.

The EC has a card operating system 550 to manage the EC's internal resources. The on-card cryptographic service 650 can be implemented in software or be provided by a cryptographic co-processor (not shown in figure 3), or other hardware solutions, or a hybrid of software and hardware.

One of the unique features of the EC is the service provider data area (SPDA) in the EC memory, which contains the service providers' account and key information. The service provider data area (SPDA) 700 contains a number of slots. In the preferred embodiment, the SPDA contains a pre-defined number (e.g. ten) of slots -- one for each potential service provider. In another embodiment, the number of slots may be dynamically changed. A record for each service provider can be placed into an empty slot. Each record contains the account number, public key, and other related information for a specific service provider.

Depending on the EC design, the SPDA can optionally allow each SP to include some software (such as an "applet" in the JAVA terminology) to manage its own on-card data and provide an interface between the SP card data and the host application. In other words, the SPDA can contain more than just simple data; it can allow each SP to put a self-contained application program (such as an applet) on the EC to provide its own unique service to the cardholder. The advantage of this type of design is that the EC itself is now detached from the type of service it can provide. Each SP can bring with it its own service capability. When another SP replaces an on-card SP, there will be no change necessary to the EC platform. The new SP applet is simply loaded into the card and it will perform what it is designed to do.

In the SPDA, each service provider is allocated space for public keys. In many transactions, only one key pair is used, but for some online transactions, two or more key pairs are required. If the SP uses the same public/private key pair for both the incoming and the signing of outgoing messages, then one public key is enough. If the SP uses a different key pair for signing, then both SP public keys (one for incoming messages and one for the signing of outgoing messages) are required in the SPDA.

In the preferred embodiment of the invention, two public/private key pairs rather than one public/private key pair is used to communicate with other applications through a network because using two public/private key pairs rather than one public/private key pair provides greater security. One pair is used for decrypting an incoming message, i.e., the sender encrypts the message using the recipient's public key and the recipient decrypts the message using the corresponding private key. The other pair is for the sender to digitally sign the message he sends out and the recipient to verify the digital signature using the corresponding sender's public.key. Each service provider is allocated space for the number of public keys used by the service provider. If the SP uses the same public/private key pair for both incoming messages and signing of outgoing messages, then one public key is enough. If the SP uses different key pairs for receiving and signing messages, then both of the SP's public keys are required in the SPDA.

In an alternative embodiment of the invention, more than two public/private key pairs may be required and used by a service provider for even greater security.

When an EC holder is issued a new financial or non-financial instrument, the issuing institution or a trusted third party will load the needed information comprising a record into an available slot. The information in the slot can be erased when the service provider account is closed. Some of the information in a slot can be read and modified during a transaction, e.g. an account balance. Some information such as account number is write protected, but can be read. Some information such as a private key is both read and write protected. The access conditions 600 contain security information such as PINs, biometric data, etc., that an EC user must submit to open the card for use or to gain access to the information stored on the card.

Traditional Personal Identification Numbers (PINs) or other security measures such as biometrics data are used to protect the EC. Biometrics involves the measurement of a cardholder's biological traits, such as physical traits and behavioral traits. A biometric system may measure an individual's fingerprints, hand-geometry, hand writing, facial appearance, speech, physical movements, keyboard typing rhythms, eye features, breath, body odor, DNA, or any other physical attribute of the cardholder. The functions provided by an EC can be activated only after all the access conditions have been satisfied. Each service provider residing on the card can optionally implement other access conditions.

Figure 4 shows the format of the service provider data area of a preferred embodiment of the invention. Each service provider's information is allocated an entry in the table, which can be protected by additional access conditions. The PIN 712 and the miscellaneous data field 714 allows the service provider to provide extra protection or data field to the instrument it supports. The name field 702 contains the names of the service providers, which can be used by the cardholder at the beginning of an online transaction to initially select the applicable service provider for a transaction. The key type field 704 specifies the type of key the service provider chooses to use, secret key, public key, etc. The key value 706 and account information fields 708 contain information unique to each service provider. The card type field 710 specifies the type of instrument a service provider supports.

In the preferred embodiment of the invention, the on-card Operating System (COS) provides some fundamental services for the cardholder. Following is a list of general functions which can be performed by the COS:

(1) Traditional OS functionality such as Memory management, task management, etc

(2) External communication-read/write of user data and communication protocol handling.

(3) Loading and updating of on-card cardholder information.

(4) User PIN changes.

(5) Service Provider Data Area management-such as loading and updating of individual service provider information, SPDA access control, etc.

The COS will also provide support during various stages of a transaction. For example, the COS can handle the SP selection at the beginning of a transaction and record the transaction into a log file when the transaction has been completed. An embodiment of the invention may implement one of the following two design approaches to the COS or a hybrid of the two design approaches:

(1) Most of the intelligence can be put into the COS whereby the COS supports most of the EC functionalities. Consequently, each on-card service provider area relies on the COS to carry out the transaction with the merchant and the SP. In this approach, the COS can provide a uniform interface with the outside world for all on-card SPs and efficiently carries out the transaction once a SP has been selected.

(2) Alternatively, the COS can be a pool of general services each on-card SP can utilize. Each SP data area can contain applets, which have the intelligence to carry out a transaction with the merchant and the SP. In this approach, the SP has more opportunity to implement its own unique feature when performing a transaction.

Figure 5 shows how digital signatures are used in the preferred embodiment of the invention. A sender of a message first prepares and sends the data portion of a message M 900 through a one way hash algorithm, H(*) 902. The output from the hash algorithm is called the message digest MD of the data portion of message M 903. The MD is then encrypted, E(MD) 904, i.e. digitally signed, using the sender's private key (Pri). The result is called the digital signature DS of a data portion of a message M. The DS is then combined with the original data portion of the message M 900 and forms a complete message 906 ready for transmission to a recipient through a network 50.

The public-key encryption/decryption function can be any of a number of encryption/decryption functions. RSA, which takes its name from the first initials of RSA developers' last names (Ronald Rivest, Adi Shamir, and Len Adelman), is just one example of a public-key encryption/decryption method, which can be used in an embodiment of the invention.

When the intended recipient receives the message from a network 50, he first separates the data portion of the message M 900 from the digital signature 912 combined with it. The recipient then runs the data portion of the message M 900 through the same hash algorithm 910 that was used to encode the data portion of message M 900, and consequently obtains a message digest MD^ 911 of the data portion of message M. The recipient then decrypts D(DS) 908 using the EC's public key, the digital signature 912 contained in the original message using the sender's public key and recovers the original message digest, denoted here as MD 909. MD 909 is compared with the new calculated MD^ 911 for correctness. If they are not identical, the original message has been corrupted and should be rejected.

Following is a list of symbols and abbreviations used in the figures 5 through 11:

Acknowledgement Data_{EC} = A part of the message sent back by the EC to the SP. It notifies the SP that the previous message has been successfully received and processed.

Acknowledgement Data_{M} = A part of the message sent back by the merchant to the SP. It notifies the SP that the previous message has been successfully received and processed.

AI_{EC} = Account information of EC holder.

AI_{M} = Account information of merchant.

CRYPTO = Cryptogram

D = Decryption function

$\mathbf{D}_{\text{SP-Private-Key}}$ = Decryption using SP's private key.

DS = Digital signature function.

$\mathbf{DS}_{\text{EC-Private-Key}}$ = Digital signature signed by the EC on a message.

$\mathbf{DS}_{\text{M-Private-Key}}$= Digital signature signed by the merchant on a message.

$\mathbf{DS}_{\text{SP-Private-Key}}$= Digital signature signed by the SP on a message.

E = Encryption function.

E (Data) = Encryption of data under a data encryption key.

$\mathbf{E}_{\text{SP-PK}}$, $\mathbf{E}_{\text{SP-Public-Key}}$ = Data encrypted by SP public key

$\mathbf{E}_{\text{Skey-EC,}}$ $\mathbf{D}_{\text{Skey-EC}}$ = Encryption/Decryption using the session key that the SP generated for the EC.

$\mathbf{E}_{\text{Skey-M,}}$ $\mathbf{D}_{\text{Skey-M}}$ = Encryption/Decryption using the session key that the SP generated for the merchant.

EC = Electronic card, or electronic card equivalent software

H (M) = Apply a one-way hashing algorithm on M. It generates the message digest (**MD**) of M.

KE = Key exchange phase.

M = Merchant

MD = Message Digest

MD^ = Message Digest produced by message recipient using the message just received as input data.

$\mathbf{MD}_{\text{EC}}$ = The message digest of a message going from EC to SP.

$\mathbf{MD}_{\text{M}}$ = The message digest of a message going from merchant to SP.

$\mathbf{MD}_{\text{SP-M}}$ = The message digest of a message going from SP to merchant.

$\mathbf{MD}_{\text{SP-EC}}$ = The message digest of a message going from SP to EC which is by passed by merchant.

PLAIN TEXT: Transaction data, which can be transmitted without encryption. Plain text can be different for different messages and transaction parties.

PLAIN TEXT_{EC} = Part of the transaction data provided by EC in its outgoing messages. Plain text data fields are not security sensitive. Therefore, they are transmitted without encryption. Note that the content of this symbol can be different when used in a different message.

PLAIN TEXT_{M} = Part of the transaction data provided by merchant in its outgoing messages. Plain text data fields are not security sensitive. Therefore, they are transmitted without encryption. Note that the content of this symbol can be different when used in a different message.

PLAIN $\text{TEXT}_{\text{SP-EC}}$ = Part of the transaction data provided by SP for EC only in its outgoing messages. Plain text data fields are not security sensitive. Therefore, they are transmitted without encryption. Note that the content of this symbol can be different when used in a different message.

PLAIN TEXT$_{SP-M}$ = Part of the transaction data provided by SP for merchant only in its outgoing messages. Plain text data fields are not security sensitive. Therefore, they are transmitted without encryption. Note that the content of this symbol can be different when used in a different message.

STD = Sensitive transaction data, which requires encryption during data transmission.

STD$_{EC}$ = Sensitive transaction digital data provided by EC in its outgoing messages. Note that the content of this symbol can be different when used in a different message.

STD$_{M}$ = Sensitive transaction digital data provided by merchant in its outgoing messages. Note that the content of this symbol can be different when used in a different message.

PK = Public key

EC-PK, PK$_{EC}$ = Public key of the electronic card.

M-PK, PK$_{M}$ = Public key of the merchant.

SP-PK, PK$_{SP}$ = Public key of the selected service provider.

Response Data$_{SP-EC}$ = A part of the message sent back by the SP to the EC during the transaction phase of a transaction. It can include approval/disapproval data and/or any other relevant data.

Response Data$_{SP-M}$ = A part of the message sent back by the SP to the merchant during the transaction phase of a transaction. It can include approval/disapproval data and/or any other relevant data.

RN = Random number.

RN$_{EC}$ = Random number generated by the EC and is sent to SP.

RN$_{SP-EC}$ = Random number generated by the SP and is sent to EC.

RN$_{M}$ = Random number generated by the merchant.

RN$_{SP-M}$ = Random number generated by the SP and is sent to M.

SP = Financial or non-financial service provider

TA = Transaction (currency) amount.

Transaction Identification Number$_{SP-EC}$, TID$_{SP-EC}$ (Transaction ID$_{SP-EC}$) = A data field whose value is assigned by the SP during the key exchange phase of a transaction. The EC will use this value to communicate with the SP during the same transaction.

Transaction Identification Number$_{SP-M}$, TID$_{SP-M}$ (Transaction ID$_{SP-M}$) = A data field whose value is assigned by the SP during the key exchange phase of a transaction. The merchant will use this value to communicate with the SP during the same transaction.

* = Combine or concatenation of data within an encryption **E** or a decryption **D.**

Figures 6A through 6Q comprise the flowchart for a preferred embodiment of the cryptographic system and method. For the purpose of simplifying the description and symbolism contained in figures 6A through 6Q, the flowchart assumes that each of the parties involved in the transaction uses one key pair. In another embodiment of the invention, two public key pairs may be used, in which case, both public keys need to be exchanged.

The preferred embodiment of the invention consists of two distinct phases: the key exchange phase and the transaction phase.

PHASE I: KEY EXCHANGE PHASE (HANDSHAKE PHASE)

The EC cardholder inserts the EC into a card read/write device or starts the EC equivalent software and enters a PIN number and/or satisfies the access conditions 110 to use the EC card. The entered security information conditions is compared 112 with the on-card information 114 to verify that user is authorized to use the EC. If the security information does not match the card security information, then the request to use the card is rejected 116. Otherwise, the card is unlocked 118 for use. Once the card is unlocked, the user can request the list of the on-card SPs available for selection and make a selection 120 by issuing an SP selection command to the EC. Once the SP is selected, the EC proceeds to start the key exchange (KE) with the SP. The public key of the selected SP, represented by the symbols SP-PK and PK$_{SP,}$ is obtained from the EC's SPDA and is used to encrypt messages that will be sent to the SP.

The main purpose of the KE is to securely send the cardholder's public key, PK$_{EC}$ 126 and an EC random number, RN$_{EC}$ 124 to the SP. The SP response to the EC is to assign a session key and a transaction ID to the EC, which will be used by the EC to communicate with the SP for the rest of the transaction. To format the KE message, the EC generates a random number, RN_{EC} 124, concatenates it with the EC's public key, PK_{EC} 126, and EC sensitive transaction data STD_{EC} 128 relevant to the transaction and/or required by the SP. The EC encrypts them 122 using the SP's public key, PK_{SP}, retrieved from the SPDA 120. The resulting EC cryptogram, $E_{ES\text{-}PK}(RN_{EC}*PK_{EC}*STD_{EC})$, is then combined 130 with the plain text portion of the message, PLAIN $TEXT_{EC}$ 132, if any, to form an EC combination message, PLAIN $TEXT_{EC}*E_{SP\text{-}PK}(RN_{EC}*PK_{EC}*STD_{EC})$. The EC's public key PK_{EC} 126 may be placed in the plain text PLAIN $TEXT_{EC}$ instead of being encrypted when forming the EC combination message.

Only sensitive data is encrypted. Non-sensitive response data is included in the plain text. Only the SP is able to read the sensitive data. In a multi-party transaction, the SP has full access to the sensitive information of all the participants.

The resulting EC combination message is then sent through a hashing algorithm 134 to form a hash message, which is the EC message digest MD_{EC}. The EC message digest MD_{EC} is digitally signed by the EC 136 using the EC private key 138 to form a digitally signed message $DS_{EC\text{-}Private\text{-}Key}$. The digitally signed message $DS_{EC\text{-}Private\text{-}Key}$ is then combined 140 with the EC combination message. The combination of the plain text PLAIN $TEXT_{EC,}$ cryptogram $CRYPTO_{EC}$ and the digital signature $DS_{EC\text{-}Private\text{-}Key}$ is the KE message from the EC and is sent to the merchant 158 through a network. Plain text includes all the transaction data fields that are not sensitive in nature and therefore can be transmitted in a clear, discernable form; they do not need to be encrypted. These data fields are different for each message and are defined by the transacting parties.

To communicate with the SP, the merchant goes through essentially the same steps to format its own KE message with the SP as the EC goes through to format the EC's KE message with the merchant. The cardholder and the merchant do not communicate with the SP individually, but through a combined message. Consequently, there will be no need to exchange any confidential financial information between the cardholder and the merchant.

The merchant prepares his device for the transaction 142 and selects from his own SPDA, which resides within the merchant's device, the same SP as the EC cardholder has selected for the transaction 144. The public key of the SP, represented by the symbols SP-PK and $PK_{SP,}$ is obtained from the SP's SPDA and is used to encrypt messages that will be sent to the SP.

To format its own KE message, the merchant generates a random number, RN_M 148, concatenates it with the merchant's public key, PK_M 150, and the merchant's sensitive transaction data $STD_{M.}$ Sensitive transaction data is data that is relevant to the transaction and/or required by the SP 152. The merchant encrypts 146 the combined data using the public key of the service provider, PK_{SP}. The resulting cryptogram is then combined 154 with the plain text portion PLAIN $TEXT_M$ 156 of the message, if any, to form a merchant combination message. The merchant's public key PK_M 150 may be placed within the plain text PLAIN $TEXT_M$ instead of being encrypted when forming the merchant combination message $\text{PLAIN TEXT}_M{*}\mathbf{E}_{SP\text{-}PK}(RN_M{*}PK_M{*}STD_M)$.

The merchant combination message $[\text{PLAIN TEXT}_M{*}\mathbf{E}_{SP\text{-}PK}(RN_M{*}PK_M{*}STD_M)]$ is further combined 158 with the EC's KE message $\{[\text{PLAIN TEXT}_{EC}{*}\mathbf{E}_{SP\text{-}PK}(RN_{EC}{*}PK_{EC}{*}STD_{EC})]{*}DS_{EC\text{-}Private\text{-}Key}\}$ to form the data portion of the KE message for both the merchant and the EC, i.e., the EC-merchant combination message $\{[\text{PLAIN TEXT}_{EC}{*}\mathbf{E}_{SP\text{-}PK}(RN_{EC}{*}PK_{EC}{*}STD_{EC})]{*}DS_{EC\text{-}Private\text{-}Key}\}{*}[\text{PLAIN TEXT}_M{*}\mathbf{E}_{SP\text{-}PK}(RN_M{*}PK_M{*}STD_M)]$. The EC-merchant combination message is sent through a hashing algorithm 160 to form a hash message, which is the merchant message digest MD_M. The merchant message digest MD_M is digitally signed 162 by the merchant using the merchant's private key 164 to form a merchant digitally signed message $DS_{M\text{-}Private\ Key}$. The merchant digitally signed message $DS_{M\text{-}Private\ Key}$ is then combined 166 with the data portion of the message, i.e., the EC-merchant combination message to form a key exchange request message $\ll \{ [\text{PLAIN TEXT}_{EC} * \mathbf{E}_{SP\text{-}PK}(RN_{EC}{*}PK_{EC}{*}STD_{EC})] * DS_{EC\text{-}Private\text{-}Key}\} * [\text{PLAIN TEXT}_M * \mathbf{E}_{SP\text{-}PK}(RN_M{*}PK_M{*}STD_M)] \gg * DS_{M\text{-}Private\text{-}Key}$ for both the merchant and EC. This final message is sent to the SP through a network. Figure 7 represents the final format and content of the key exchange request message from a merchant to an SP.

In the preferred embodiment of the invention, the merchant does not check the MD of the EC's request message MD_{EC} because the EC encrypts his public key. However, in an alternate embodiment of the invention, if the EC chooses not to encrypt his public key then the merchant can optionally check the EC's MD before passing it to the SP. In either the case where the EC encrypts his public key or where the EC does not encrypt his public key, for enhanced security and to avoid possible processing errors by the merchant, the SP can still check the EC's MD. When the merchant receives a combination response from the SP for both himself and the EC, the merchant does not have to check the MD for the EC since it is part of the overall message formed by a single originator -- the SP. The merchant only needs to check the MD of the overall message he receives from the SP.

When the SP receives the KE request message, the SP first separates 168 the data portion of the KE request message from the DS and feeds the data portion of the KE request message into a one-way hash algorithm to recalculate the message digest, which becomes MD_M. The SP then separates the merchant's plain text PLAIN $TEXT_M$, cryptogram $CRYPTO_M$, digital signature $DS_{M\text{-Private-Key}}$ and the EC's KE request message PLAIN $TEXT_{EC}$*$CRYPTO_{EC}$ *$DS_{EC\text{-Private-Key}}$. Using its own private key, the SP decrypts merchant's cryptogram 170 and recovers, among other information, the merchant's random number RN_M 148 and the merchant's public key PK_M 150. The SP then uses the recovered PK_M to decrypt the digital signature signed by the merchant $DS_{M\text{-Private-Key}}$ and recovers the MD_M for the merchant's KE message. The SP compares 172 the newly hashed $MD^\wedge_M$ 168 with the MD_M 170 recovered by decrypting the DS from the original KE message. If there is a discrepancy between $MD^\wedge_M$ and MD_M found, then the KE message has been corrupted and is therefore rejected 174. If $MD^\wedge_M$ and MD_M match, then the SP separates the data portion of the EC's KE request message from the DS and feeds the data portion of the EC's KE request message into a one-way hash algorithm to recalculate the message digest ($MD^\wedge_{EC}$). The SP then separates the EC's plain text PLAIN $TEXT_{EC}$, if any, cryptogram $CRYPTO_{EC}$, and digital signature $DS_{EC\text{-Private Key}}$, in the data portion of the EC's KE request message 176. Using its own private key, the SP decrypts EC's cryptogram and recovers, among other information, EC's random number RN_{EC} and EC's public key PK_{EC} . The SP then uses the recovered PK_{EC} to decrypt the digital signature signed by EC and recovers the MD_{EC} for EC's KE message. In the step 178, SP compares the newly hashed $MD^{\wedge}_{EC}$ 176 with the MD_{EC} recovered by decrypting the DS from the original KE message. If there is any discrepancy found, the KE message has been corrupted and is therefore rejected 180. Otherwise, SP is ready to send a KE response message back to merchant and EC.

To format the KE response message for the EC, the SP generates a random number, $RN_{SP\text{-}EC}$ 184, and a session key $Skey_{EC}$ 186 for the EC, combines them with the EC generated random number, 188 RN_{EC}, service provider sensitive transaction data $STD_{SP\text{-}EC}$ 190 and encrypts them 192 using the EC's public key PK_{EC}. The resulting cryptogram, $\mathbf{E}_{EC\text{-}PK}(RN_{EC}*RN_{SP\text{-}EC}*Skey_{EC}*STD_{SP\text{-}EC})$, is combined 196 with a transaction identification number, $TID_{SP\text{-}EC}$ 194 assigned to the EC by the SP and plain text, PLAIN $TEXT_{SP\text{-}EC}$ 195, if any, to form the data portion of the response message for the EC. The SP runs this data through a hash algorithm to calculate the message digest $MD_{SP\text{-}EC}$ 198. Using its own private key 202, the SP creates a digital signature $DS_{SP\text{-}Private\text{-}Key}$ 200 for the response message by digitally signing the message digest $MD_{SP\text{-}EC}$. After combining 204 the data portion of the message with the newly calculated $DS_{SP\text{-}Private\text{-}Key}$, the SP's KE response message for the EC is complete, $[TID_{SP\text{-}EC}$*PLAIN $TEXT_{SP\text{-}EC}*\mathbf{E}_{EC\text{-}PK}(RN_{SP\text{-}EC}*RN_{EC}*Skey_{EC}*STD_{EC})]*DS_{SP\text{-}Private\text{-}Key}$.

To format the KE response message for the merchant, the SP generates a random number $RN_{SP\text{-}M}$ 208 and a session key $Skey_{M}$ 210 for the merchant and combines them with the merchant generated random number RN_{M} 212, sensitive transaction data $STD_{SP\text{-}EC}$ 214 and encrypts them 206 using the merchant's public key PK_{M} recovered in 170. The resulting cryptogram is combined 216 with a transaction identification number, $TID_{SP\text{-}M}$ 218, assigned to the merchant by the SP and plain text, PLAIN $TEXT_{SP\text{-}M}$ 220, if any, to form the data portion of the response message for merchant. The resulting combination message, $TID_{SP\text{-}M}$*PLAIN $TEXT_{SP\text{-}M}*\mathbf{E}_{M\text{-}PK}(RN_{SP\text{-}M}*RN_{M}*Skey_{M}*STD_{SP\text{-}M})$ is further combined 222 with the KE response message for the EC, $[TID_{SP\text{-}EC}$*PLAIN $TEXT_{SP\text{-}EC}*\mathbf{E}_{EC\text{-}PK}(RN_{SP\text{-}EC}*RN_{EC}*Skey_{EC}*STD_{EC})]*DS_{SP\text{-}Private\text{-}Key}$, to form the data portion of the SP's final KE response message, $[TID_{SP\text{-}EC}$*PLAIN $TEXT_{SP\text{-}EC}*\mathbf{E}_{EC\text{-}PK}*(RN_{SP\text{-}}$

$_{\text{EC}}*\text{RN}_{\text{EC}}*\text{Skey}_{\text{EC}}*\text{STD}_{\text{EC}})]*\text{DS}_{\text{SP-Private-Key}}*[\text{TID}_{\text{SP-M}}*\text{PLAIN TEXT}_{\text{SP-M}}*\mathbf{E}_{\text{M-PK}}(\text{RN}_{\text{SP-M}}*\text{RN}_{\text{M}}*\text{Skey}_{\text{M}}*\text{STD}_{\text{SP-M}})]$. The SP runs the data portion through a hash algorithm to calculate the message digest 224. Using its own private key 228, the SP creates a digital signature, $\text{DS}_{\text{SP-Private-Key}}$ 226, for the response message by digitally signing the message digest. After combining 230 the data portion of the message with the newly calculated DS 226, the KE response message for both the EC and the merchant is complete. The response message $<<\{[\text{TID}_{\text{SP-EC}}*\text{PLAIN TEXT}_{\text{SP-EC}}*(\mathbf{E}_{\text{EC-PK}}*\text{RN}_{\text{SP-EC}}*\text{RN}_{\text{EC}}*\text{Skey}_{\text{EC}}*\text{STD}_{\text{SP-EC}})]*\text{DS}_{\text{SP-Private-Key}}\}*[\text{TID}_{\text{SP-M}}*\text{PLAIN TEXT}_{\text{SP-M}}*\mathbf{E}_{\text{M-PK}}(\text{RN}_{\text{SP-M}}*\text{RN}_{\text{M}}*\text{Skey}_{\text{M}}*\text{STD}_{\text{SP-M}})]>>\text{DS}_{\text{SP-Private-Key}}$ is sent back to the merchant through a network. Figure 8 depicts the final format and content of the combined KE response message from the SP to the merchant.

When the merchant receives the KE response message 232, the merchant first separates the $\text{DS}_{\text{SP-Private-Key}}$, which was signed by the SP, and then feeds the data portion of the combined KE response message into a one-way hash algorithm to recalculate the message digest $\text{MD}^{\wedge}_{\text{SP-M}}$. The merchant then separates the data portion of the SP's KE response message, i.e., $\text{TID}_{\text{SP-M}}$, $\text{PLAIN TEXT}_{\text{SP-M}}$, $\text{CRYPTO}_{\text{SP-M}}$, $[(\text{TID}_{\text{SP-EC}}*\text{PLAIN TEXT}_{\text{SP-EC}}*\text{CRYPTO}_{\text{SP-EC}})]*\text{DS}_{\text{SP-Private-Key}}$. The merchant uses SP's public key (selected from 144) to decrypt the digital signature $\text{DS}_{\text{SP-Private-Key}}$ to recover the message digest $\text{MD}_{\text{SP-M}}$. The merchant compares 234 the newly hashed $\text{MD}^{\wedge}_{\text{SP-M}}$ with the $\text{MD}_{\text{SP-M.}}$ If there is any discrepancy between $\text{MD}^{\wedge}_{\text{SP-M}}$ and $\text{MD}_{\text{SP-M}}$, the KE response message has been corrupted and is therefore rejected 236. If $\text{MD}^{\wedge}_{\text{SP-M}}$ and $\text{MD}_{\text{SP-M}}$ match, then the merchant identifies the part of the response message which is meant for him and decrypts the cryptogram $\text{CRYPTO}_{\text{SP-M}}$ 238 using his own private key. The merchant should be able to recover the original random number RN_{M} (of 148) that he sent to the SP in the KE request message. The merchant compares 240 the recovered random number RN_{M} (of the step 238) with the original random number RN_{M}. If they are not equal, then the message has been corrupted and the message is rejected 242. Since the random number RN_{M} can only be recovered by the SP using the correct SP private key, it is assured that the sender of the message is indeed the selected SP. The merchant then forwards the EC's KE response message $[(\text{TID}_{\text{SP-EC}}*\text{PLAIN TEXT}_{\text{SP-EC}}*\text{CRYPTO}_{\text{SP-EC}})]*\text{DS}_{\text{SP-Private-Key}}$ to the EC and prepares for the transaction phase of the transaction.

When the EC receives the KE response message 260, the EC first separates the $DS_{SP-Private-Key}$, which was signed by the SP, and then feeds the data portion of the KE response message for the EC into a one-way hash algorithm producing a $MD\hat{}_{SP-EC}$. The EC then separates the data portion of the message, i.e., TID_{SP-EC}, PLAIN $TEXT_{SP-EC}$, $CRYPTO_{SP-EC}$, $DS_{SP-Private-key}$. The EC uses SP's public key (selected in 120) to decrypt the digital signature $DS_{SP-Private-key}$ message and recovers the message digest MD_{SP-EC}. The EC compares 262 the newly hashed $MD\hat{}_{SP-EC}$ (in 260) with the MD_{SP-EC} recovered by decrypting the $DS_{SP-Private-key}$ from the KE response message for EC. If there is any discrepancy between $MD\hat{}_{SP-EC}$ and MD_{SP-EC} found, the KE response message for the EC has been corrupted and is therefore rejected 264. If $MD\hat{}_{SP-EC}$ and MD_{SP-EC} match, the EC identifies the part of the response message which is meant for him and decrypts 266 the cryptogram $CRYPTO_{SP-EC,}$ which is contained in the message, using his own private key. The EC should be able to recover the original random number RN_{EC} (of 124) that was sent in the EC KE request message. The EC compares 268 the recovered random number RN_{EC} (of 266) with the original random number RN_{EC} (of 124). If the random numbers are not equal, then the message has been corrupted and the message is rejected 270. Since only the SP using the correct SP private key can recover the random number RN_{EC}, this serves to ensure that the sender of the message is indeed the selected SP. The EC prepares for the transaction phase of the transaction.

There will be a predefined timeout period set in the EC and the merchant. During a transaction, if a response message is not received within a timeout period, the EC and the merchant will consider the transaction aborted and will either retry or start the recovery process.

After successful completion of the KE message exchanges, the SP has EC's public key and the merchant's public key. At this point, both the EC and the merchant has a random number, a transaction ID, and a session key from the SP. The EC and the merchant must send the two random numbers recovered from the KE response message back to the SP to complete the key exchange phase of the transaction. This can be done in two ways. The random numbers can be sent back through a confirmation message from both the EC and the merchant. Or the random numbers can be sent back as part of the next message going out from the EC and the merchant to the SP, such as a transaction message. The second method is simpler and is described in phase II below. The random numbers are used only once to ensure the correctness of the key exchange between the SP and merchant, and the SP and EC. Once the session keys and transaction identification number have been established, the random number are no longer be used.

PHASE II: TRANSACTION PHASE

During the transaction phase, the merchant and the EC each sends their own account information such as an account number and other transaction related data such as transaction amount, request for approval or other processing, to the SP. Again, the EC and the merchant talk to the SP individually but through combined messages and the merchant is responsible for combining the messages and sending them as one message to the SP.

The EC first forms the transaction message by concatenating the random number $RN_{SP\text{-}EC}$ 274 from the SP and the EC's account information with the selected SP, AI_{EC} 276, transaction amount TA 280 and any other sensitive data 278 relevant to the transaction and/or required by the SP. The EC encrypts 272 them using the session key $Skey_{EC}$ assigned by the SP. The $Skey_{EC}$ is a secret key and uses a cryptographic algorithm different from the cryptographic algorithm used for the public key encryption. The resulting cryptogram $CRYPTO_{EC}$, i.e., $Skey_{EC}(RN_{SP\text{-}EC}*STD_{EC}*AI_{EC}*TA)$, is then combined 282 with the transaction ID $TID_{SP\text{-}EC}$ 284 and the plain text PLAIN $TEXT_{EC}$286, if any, to form the data portion of the EC's transaction message, $TID_{SP\text{-}EC}$*PLAIN $TEXT_{EC}*CRYPTO_{EC}$. The data portion 282 is fed into a one-way hash algorithm 288 to calculate the message digest MD_{EC} and the MD_{EC} is then digitally signed 290 by the EC's private key 292. The resulting digital signature 290 is combined with the data portion of the message (from 282) 294 to form EC's transaction request message and then sent to the merchant, $[TID_{SP\text{-}EC}$*PLAIN $TEXT_{EC}*Skey_{EC}(RN_{SP\text{-}EC}*STD_{EC}*AI_{EC}*TA)]*DS_{EC\text{-}Private\text{-}Key}$.

The merchant goes through essentially the same steps to form his transaction message. The merchant forms his transaction message by concatenating 246 the $RN_{SP\text{-}M}$ from the SP and the merchant's account information with the selected SP, AI_M 248, transaction amount

TA 252 and any other sensitive data STD_M 250 relevant to the transaction and/or required by the SP. The merchant encrypts them 244 using the session key $Skey_M$ assigned by the SP. The session key $Skey_M$ is a secret key and is created using a different cryptographic algorithm, such as DES, from the cryptographic algorithm used for public key encryption. The session key $Skey_M$ is used to perform the encryption at this point to create the cryptogram $CRYPTO_M$. The resulting cryptogram $CRYPTO_M$, i.e., $Skey_M(RN_{SP\text{-}M}*STD_M*AI_M*TA)$, is then combined 254 with the transaction ID $TID_{SP\text{-}M}$ 256 and the plain text PLAIN $TEXT_M$ 258, if any, to form the data portion of the merchant's transaction message, $TID_{SP\text{-}M}*PLAIN\ TEXT_M*CRYPTO_M$. This data is combined 296 with the EC's transaction request to form the data portion of the final transaction request message for the SP, $[TID_{SP\text{-}EC}*PLAIN\ TEXT_{EC}*Skey_{EC}(RN_{SP\text{-}EC}*STD_{EC}*AI_{EC}*TA)]*DS_{EC\text{-}Private\text{-}Key}*[TID_{SP\text{-}M}*PLAIN\ TEXT_M*Skey_M(RN_{SP\text{-}M}*STD_M*AI_M*TA)]$. As before, the merchant feeds his combined data through a one-way hash algorithm 298 to calculate the message digest MD_M and the MD_M is then digitally signed 300 by the merchant's private key 302. The resulting digital signature $DS_{M\text{-}Private\text{-}Key}$ 300 is combined 304 with the data portion of the message (from 296) to form the final transaction request message and is then sent to the SP, $\{[TID_{SP\text{-}EC}*PLAIN\ TEXT_{EC}*Skey_{EC}(RN_{SP\text{-}EC}*STD_{EC}*AI_{EC}*TA)]*DS_{EC\text{-}Private\text{-}Key}*[TID_{SP\text{-}M}*PLAIN\ TEXT_M*Skey_M(RN_{SP\text{-}M}*STD_M*AI_M*TA)]\}*DS_{M\text{-}Private\text{-}Key}$. Figure 9 depicts the final format of the transaction request message.

When the SP receives the transaction request message, the SP first checks 306 the two transaction identification numbers, i.e., $TID_{SP\text{-}EC}$ and $TID_{SP\text{-}M}$, sent by the EC and the merchant and makes sure they are valid. When either $TID_{SP\text{-}M}$ (of 218) or $TID_{SP\text{-}EC}$ (of 194) is found invalid 306, then the message is rejected 308. If the transaction identification numbers are both valid, then the SP proceeds to separate the $DS_{M\text{-}Private\text{-}Key}$ from the data portion of the message and feeds the data portion of the message, $\{[TID_{SP\text{-}EC}*PLAIN\ TEXT_{EC}*Skey_{EC}(RN_{SP\text{-}EC}*STD_{EC}*AI_{EC}*TA)]*DS_{EC\text{-}Private\text{-}Key}*[TID_{SP\text{-}M}*PLAIN\ TEXT_M*Skey_M(RN_{SP\text{-}M}*STD_M*AI_M*TA)]\}$ into a one-way hash algorithm to calculate the message digest $MD^{\wedge}_M$ of this message. The SP separates the data portion of the message, i.e., $TID_{SP\text{-}M}$, PLAIN $TEXT_M$,$CRYPTO_M$, $DS_{M\text{-}Private\text{-}Key}$, $(TID_{SP\text{-}EC}*PLAIN\ TEXT_{EC}*CRYPTO_{EC})*DS_{EC\text{-}Private\text{-}Key}$. The

SP decrypts 310 the $DS_{M\text{-Private-Key}}$ using the merchant's public key and compares the newly recovered message digest MD_M with the message digest just calculated $MD^\wedge_M$ (from 306). If $MD^\wedge_M$ and MD_M are not equal, the message has been corrupted and is rejected 314. If $MD^\wedge_M$ and MD_M match, then the SP decrypts 316 the encrypted portion of the message using the session key $Skey_M$ (of 210) it assigned to the merchant during the KE phase and recovers the data fields contained in the encrypted portion. The SP compares 318 the random number $RN_{SP\text{-}M}$ the merchant sends back in the message with the message the SP sent to the merchant originally, $RN_{SP\text{-}M}$ (from 208). If the random numbers are not equal, then the merchant has failed the mutual authentication test and the message is rejected 320.

In addition, the SP will verify the EC's account information AI_{EC} and the transaction data such as the transaction amount TA. The message is rejected 320 if the AI is no longer valid. It is also rejected when the TA from the EC and the TA from the merchant do not match. There may be other conditions for invalidating a message. If the account information AI_{EC} and the transaction are valid, then the SP goes on to verify the EC portion of the message.

As with the merchant's message, the SP first separates 322 the $DS_{EC\text{-Private-Key}}$ from the EC's message and feeds the data portion of the EC's message, ($TID_{SP\text{-}EC}$*PLAIN $TEXT_{EC}$*$CRYPTO_{EC}$) into a one-way hash algorithm to calculate the message digest $MD^\wedge_{EC}$ of the EC message. The SP separates the data portion of EC's transaction request, $TID_{SP\text{-}EC}$, PLAIN $TEXT_{EC}$, $CRYPTO_{EC}$, $DS_{EC\text{-Private-Key}}$. The SP decrypts 324 $DS_{EC\text{-Private-Key}}$ using EC's public key PK_{EC} and recovers MD_{EC}. The SP compares 326 the recovered MD_{EC} with $MD^\wedge_{EC}$. If $MD^\wedge_{EC}$ and MD_{EC} are not equal, the message has been corrupted and is rejected 328. If $MD^\wedge_{EC}$ and MD_{EC} match, then the SP decrypts 330 the encrypted portion of the EC message using the session key $Skey_{EC}$ (of 186) it assigned to the EC during the KE phase and recovers the data fields contained in it. The SP compares 332 the random number $RN_{SP\text{-}EC}$ the EC sends back in the message with the random number $RN_{SP\text{-}EC}$ it sent out to the EC originally (in 184). If the random numbers are not equal, then the EC has failed the mutual authentication test and the message is rejected 334. The SP will verify the merchant's account information AI_M and the transaction data such as the transaction amount TA and will reject the message when the account information is invalid or when the transaction data does not meet the SP's criterion 334. Once the integrity and authenticity of the overall message has been established, the SP can process the data contained in the message and send a response message back. The random number that is sent back in this message completes the mutual authentication between the SP and the merchant, and between the SP and the EC. After this message, no exchange of random numbers will be necessary. The SP can chooses to use the random number as the transaction identification number which the merchant and the EC will use in all subsequent messages that they send to the SP.

As before, the response message contains information for both the EC and the merchant. To format the transaction response message for the EC, the SP generates the response data for the EC, Response $\text{Data}_{\text{SP-EC}}$ 338, and encrypts 336 it using the session key Skey_{EC} assigned to the EC. Only sensitive data is encrypted. Non-sensitive response data is included in the plain text. The cryptogram $\text{CRYPTO}_{\text{SP-EC}}$, i.e., $\mathbf{E}_{\text{Skey-EC}}$(Response $\text{Data}_{\text{SP-EC}}$), is combined 340 with the transaction identification number $\text{TID}_{\text{SP-EC}}$ 342 that the SP assigned to the EC (from 194) and the plain text that the SP has for EC 344, if any, to form the data portion of the response message for the EC, i.e., $\text{TID}_{\text{SP-EC}}$*PLAIN $\text{TEXT}_{\text{SP-EC}}$*$\mathbf{E}_{\text{Skey-EC}}$(Response $\text{Data}_{\text{SP-EC}}$). The data portion of the message is fed into a hash algorithm 346 to generate a $\text{MD}_{\text{SP-EC}}$ which is digitally signed 348 by the SP using the SP's private key 350. The $\text{DS}_{\text{SP-Private-Key}}$ is combined 352 with the data portion of the response message (from 340) to form the complete response message for the EC, [$\text{TID}_{\text{SP-EC}}$*PLAIN $\text{TEXT}_{\text{SP-EC}}$*$\mathbf{E}_{\text{Skey-EC}}$(Response $\text{Data}_{\text{SP-EC}}$)]*$\text{DS}_{\text{SP-Private-Key}}$. To format the transaction response message for the merchant, the SP generates the response data for the merchant, Response $\text{Data}_{\text{SP-M}}$ 356, and encrypts 354 it using the session key Skey_{M} assigned to the merchant (from 210). The cryptogram $\text{CRYPTO}_{\text{SP-M}}$, is combined 358 with the transaction identification number $\text{TID}_{\text{SP-M}}$ assigned to merchant 360 (from 218) and the plain text PLAIN $\text{TEXT}_{\text{SP-M}}$ that the SP has for merchant 362, if any, to form the data portion of the response message for the merchant, $\text{TID}_{\text{SP-M}}$*PLAIN $\text{TEXT}_{\text{SP-M}}$*$\text{CRYPTO}_{\text{SP-M}}$. The data is then combined 364 with the completed response message for the EC to form the data portion of the response message for both the EC and the merchant, [($\text{TID}_{\text{SP-EC}}$*PLAIN $\text{TEXT}_{\text{SP-EC}}$*$\mathbf{E}_{\text{Skey-EC}}$(Response $\text{Data}_{\text{SP-EC}}$)]*$\text{DS}_{\text{SP-Private-Key}}$*[$\text{TID}_{\text{SP-M}}$*PLAIN $\text{TEXT}_{\text{SP-M}}$*$\mathbf{E}_{\text{Skey-M}}$(Response $\text{Data}_{\text{SP-M}}$)].

The data is then fed into a hash algorithm 366 to generate a MD_{SP-M} which is digitally signed 368 by the SP using the SP's private key 370. The $DS_{SP-Private-Key}$ is combined 372 with the data portion of the response message for both the EC and the merchant to form the complete response message for both the EC and the merchant, <<{[TID_{SP-EC}*PLAIN $TEXT_{SP-EC}$*$\mathbf{E}_{Skey-EC}$(Response $Data_{SP-EC}$)]*$DS_{SP-Private-Key}$}*[TID_{SP-M}*PLAIN $TEXT_{SP-M}$*$\mathbf{E}_{Skey-M}$(Response $Data_{SP-M}$)]>>*$DS_{SP-Private-Key}$. The SP then sends its response message back to the merchant. Figure 10 depicts the final format of the transaction response message.

When the merchant receives the message, the merchant first checks 374 the transaction identification number, $TID_{SP-M,}$ in the message and makes sure it is valid. If the transaction identification number is invalid then the message is rejected 376. If the TID_{SP-M} is valid, then the merchant separates the $DS_{SP-Private-Key}$ which was signed by the SP from the data portion of the message, and then feeds the data portion of the transaction response message <<{[TID_{SP-EC}*PLAIN $TEXT_{SP-EC}$*$\mathbf{E}_{Skey-EC}$(Response $Data_{SP-EC}$)]*$DS_{SP-Private-Key}$}*[TID_{SP-M}*PLAIN $TEXT_{SP-M}$*$\mathbf{E}_{Skey-M}$(Response $Data_{SP-M}$)]>> into a one-way hash algorithm producing a $MD^\wedge_{SP-M}$. The merchant separates the data portion of the message into different parts, TID_{SP-M}, PLAIN $TEXT_{SP-M}$, $CRYPTO_{SP-M}$, $DS_{SP-Private-Key}$ (TID_{SP-EC}*PLAIN $TEXT_{SP-EC}$*$CRYPTO_{SP-EC}$*$DS_{SP-Private-Key}$) and prepares to forward SP's transaction response message to the EC. The merchant decrypts 378 the encrypted portion of the SP's message using the session key $Skey_M$ assigned by the SP during the KE phase and recovers the data fields contained within it. The merchant then uses SP's public key, PK_{SP} (from144), to decrypt the digital signature $DS_{SP-Private-Key}$ to recover MD_{SP-M}. The merchant compares 380 the newly hashed $MD^\wedge_{SP-M}$ (from 374) with the recovered $MD_{SP-M.}$ If $MD^\wedge_{SP-M}$ and MD_{SP-M} do not match, then the transaction response message has been corrupted and is therefore rejected 382. If the message digests match, then the merchant starts processing the message. As usual, the EC portion of the transaction response message (TID_{SP-EC}*PLAIN $TEXT_{SP-EC}$*$CRYPTO_{SP-EC}$*$DS_{SP-Private-Key}$) is passed to EC.

When the EC receives the transaction response message, the EC first checks 394 the transaction identification number, $TID_{SP-EC,}$ in the message and makes sure it is valid. If the transaction identification numbers is invalid, then the message is rejected 396. If the transaction identification number is valid, then the merchant separates the $DS_{SP\text{-}Private\text{-}Key}$ which was signed by the SP, from the data portion of the transaction response message, and then feeds the data portion of the EC transaction response message $TID_{SP\text{-}EC}$*PLAIN $TEXT_{SP\text{-}EC}$*$\mathbf{E}_{Skey\text{-}EC}$(Response $Data_{SP\text{-}EC}$) into a one-way hash algorithm producing $MD\hat{}_{SP\text{-}EC}$. The EC separates the message into different parts, $TID_{SP\text{-}EC}$, $PLAINT_{SP\text{-}EC}$, $CRYPTO_{SP\text{-}EC}$, $DS_{SP\text{-}Private\text{-}Key}$. The EC decrypts 398 the encrypted portion of SP's message using the session key Skey assigned by the SP during the KE phase and recovers the data fields contained within it. The EC uses SP's public key (from 120) to decrypt the digital signature $DS_{SP\text{-}Private\text{-}Key}$ and recovers the message digest $MD_{SP\text{-}EC}$. The merchant compares 400 the newly hashed $MD\hat{}_{SP\text{-}EC}$ 394 with the recovered $MD_{SP\text{-}EC}$. If $MD\hat{}_{SP\text{-}EC}$ and $MD_{SP\text{-}EC}$ do not match, then the transaction response message has been corrupted and is therefore rejected 402. If the message digests match, then the EC starts processing the message.

At the end of the transaction, the EC and the merchant can, if required by the SP, send an acknowledgement message to the SP to signal that the response message has been correctly received and processed. This acknowledgement data can be included as a part of the next message to be sent to the SP, if there are more messages to be exchanged between the SP and the merchant and the EC before the transaction ends. Or the acknowledgement data can be a message by itself.

To format the acknowledgement message, the EC first encrypts 404 the sensitive part of the acknowledgement data, Acknowledgement $Data_{EC}$, 406, if any, using the session key, $Skey_{EC}$, thus creating $Skey_{EC}$(Acknowledgement $Data_{EC}$). The EC combines 408 the resulting cryptogram with the transaction identification number $TID_{SP\text{-}EC}$ 410 assigned by the SP and the plain text PLAIN $TEXT_{EC}$ 412, if any. This forms the data portion of EC's acknowledgement message, $TID_{SP\text{-}EC}$*PLAIN $TEXT_{EC}$* $Skey_{EC}$(Acknowledgement $Data_{EC}$). This combined data is then fed into a one-way hash algorithm 414 to generate the MD_{EC}. The resulting MD_{EC} is then digitally signed 416 by the EC using the EC's private key 418 to generate a $DS_{EC\text{-}Private\text{-}Key}$. The DS $_{EC\text{-}Private\text{-}Key}$ is combined 420 with the data portion of the message (from 408) to form the complete acknowledgement message for the EC, [$TID_{SP\text{-}}$

$_{EC}$*PLAIN TEXT$_{EC}$*Skey$_{EC}$(Acknowledgement Data$_{EC}$)]*DS$_{Ec\text{-}Private\text{-}Key}$. The acknowledgement message is then sent to the merchant.

The merchant goes through the same steps to form his own acknowledgement message. To format the acknowledgement message, the merchant first encrypts the sensitive parts of the acknowledgement data, Acknowledgement Data$_M$ 386, if any using the session key Skey$_M$ assigned by the SP to merchant, thus creating Skey$_M$(RN$_{SP\text{-}M}$*Acknowledgement Data$_M$). The merchant combines 388 the resulting cryptogram with the transaction identification number TID$_{SP\text{-}M}$ 390 assigned by the SP, and the plain text PLAIN TEXT$_M$ (from 392), if any. This forms the data portion of the merchant's acknowledgement message, TID$_{SP\text{-}M}$*PLAIN TEXT$_M$* Skey$_M$(RN$_{SP\text{-}M}$*Acknowledgement Data$_M$). This data portion is further combined 422 with the acknowledgement message received from the EC to form the data portion of the combined acknowledgement message for the SP, {[TID$_{SP\text{-}EC}$*PLAIN TEXT$_{EC}$*Skey$_{EC}$(Acknowledgement Data$_{EC}$)]*DS$_{EC\text{-}Private\text{-}Key}$}*[TID$_{SP\text{-}M}$*PLAIN TEXT$_M$*Skey$_M$(Acknowledgement Data$_M$)]. The merchant feeds the data portion of the combined acknowledgement message for the SP into a one-way hash algorithm to generate the message digest MD$_M$. The resulting MD$_M$ is then digitally signed by the merchant using the merchant's private key 428 to generate DS$_{M\text{-}Private\text{-}Key}$ 426. The DS$_{M\text{-}Private\text{-}Key}$ is combined 430 with the data portion of the message (from 422) to form the final combined acknowledgement message of the EC and the merchant designated for the SP, <<{[TID$_{SP\text{-}EC}$*PLAIN TEXT$_{EC}$*Skey$_{EC}$(Acknowledgement Data$_{EC}$)]*DS$_{EC\text{-}Private\text{-}Key}$}*[TID$_{SP\text{-}M}$*PLAIN TEXT$_M$*Skey$_M$(Acknowledgement Data$_M$)]>>*DS$_{M\text{-}Private\text{-}Key}$. This message is then sent to the SP. Figure 11 depicts the final format of the transaction acknowledgement message.

TID$_{SP\text{-}M}$ is the transaction identification number assigned by the SP to the merchant (from 218) and TID$_{SP\text{-}EC}$ is the transaction identification number assigned by the SP to the EC (from 194). Upon receiving the transaction acknowledgement message, the SP checks 432 the two transaction identification numbers, TID$_{SP\text{-}M}$ and TID$_{SP\text{-}EC}$, sent by the EC and the merchant and makes sure they are valid. When either TID$_{SP\text{-}M}$ or TID$_{SP\text{-}EC}$ is found invalid, then the message is rejected 434. If the transaction identification numbers are both valid, then the SP proceeds to separate the DS$_{M\text{-}Private\text{-}Key}$ from the combined acknowledgement message and feeds the data portion of the combined acknowledgement message <<{[TID_{SP-EC}*PLAIN $TEXT_{EC}$*$Skey_{EC}$(Acknowledgement $Data_{EC}$)]*$DS_{EC-Private-Key}$}*[TID_{SP-M}*PLAIN $TEXT_{M}$*$Skey_{M}$(Acknowledgement $Data_{M}$)]>> into a one-way hash algorithm to calculate the message digest $MD^{\wedge}_{M}$ of this message. The SP separates the data portion of the message, TID_{SP-M}, PLAIN $TEXT_{M}$, $CRYPTO_{M}$, $DS_{M-Private-Key}$, (TID_{SP-EC}*PLAIN $TEXT_{EC}$*$CRYPTO_{EC}$)*$DS_{EC-Private-Key}$. The SP decrypts 436 the $DS_{M-Private-Key}$ using the merchant's public key PK_{M} and compares the recovered message digest MD_{M} 432 with the message digest just calculated $MD^{\wedge}_{M}$ 436. If $MD^{\wedge}_{M}$ and MD_{M} are not equal, then the message has been corrupted and is rejected 440. If $MD^{\wedge}_{M}$ and MD_{M} match, then the SP decrypts 442 the encrypted portion of the merchant's acknowledgement message using the session key $Skey_{M}$ (from 210) that it assigned to the merchant during the KE phase and recovers the acknowledgement data contained within it.

The SP separates 444 the $DS_{EC-Private-Key}$ from the EC's acknowledgement message and feeds the data portion of the EC's acknowledgement message, TID_{SP-EC}*PLAIN $TEXT_{EC}$*$CRYPTO_{EC}$, into a one-way hash algorithm to calculate the message digest $MD^{\wedge}_{EC}$ of this message. The SP separates the data portion of the EC's acknowledgement message, TID_{SP-EC}, PLAIN $TEXT_{EC}$, $CRYPTO_{EC}$, $DS_{EC-Private-Key}$. The SP decrypts 446 the $DS_{EC-Private-Key}$ using the EC's public key PK_{EC} and compares 448 the recovered MD_{EC} with the message digest just calculated $MD^{\wedge}_{EC}$ 444. If the message digests are not equal, then the message has been corrupted and is rejected 450. If $MD^{\wedge}_{EC}$ and MD_{EC} match, then the SP decrypts 452 the encrypted portion of the message using the session key $Skey_{EC}$ (from 186) that it assigned to the EC during the KE phase and recovers the acknowledgement data contained within it. This completes the processing of the transaction phase of the transaction 454.

Throughout the transaction, in a preferred embodiment, the EC works with interface software provided by Internet browser software such as the Microsoft Explorer or Netscape Navigator. In a typical session, the cardholder points his browser to the merchant's URL and orders goods or services from the merchant. At the time of payment, the browser will invoke the EC interface software, which can be built into the browser or included as a plug-in or add-on software component, and allow the transaction to proceed. The cardholder can point his browser to the URL of any SP member.

The two-phased transaction described in figure 6A-6Q above is just a specific case of applying the two-phased key-exchange-transaction model. In the two-phased transaction described in figures 6A-6Q, the number of parties involved in the transaction is three: the EC, the merchant and the SP. The two-phased key-exchange-transaction model is similarly applicable to cases where the number of parties involved varies from two to many. In a transaction that involves more than three parties, there is only one party that plays the role of the SP. All other parties use the public key of the selected SP to perform the initial key exchange and use session keys and transaction Ids assigned by the SP to carry out the transaction.

The two-phased key-exchange-transaction model is applicable to organization schemes wherein: (1) the participants can be arranged with possible routers in series with the service provider; or (2) the participants can be arranged with possible routers in a hierarchical organization. These additional organization schemes may involve routers, which route messages to the next level. A level of a hierarchy may be composed of any number of participants and/or routers. The next level is the next participant or router that is next in the sequence or hierarchy. In a hierarchical organization scheme, the next level includes all possible next participants and routers. For the hierarchical organization scheme, the SP establishes the criterion for determining the next participant or router to which a message is sent.

A router is a gateway/conduit, which collects the messages from a previous level and performs some processing on the messages according to an SP's requirements such as combining them, and then forwards the messages to the SP. Each participant need only form his own message (data and digital signature) and send it to the next level. A participant combines all the messages he receives with his own message and digitally signs the combined message before sending it to next level. In the hierarchical organization's simplest form, there is only one message router, which collects messages from all the other participants and sends the combined message to the SP.

In the series organization, an originator of a transaction is in series with routers and/or participants who in turn are in series with a service a service provider 60. In the preferred embodiment of the invention, each element shown in figure 12 is a participant. In an alternative embodiment of the invention, any intermediate element between the originator and the SP can be a router.

An originator conducts a transaction with participants 1100, 1120, 1140 and1160 and a service provider that have been arranged in series as shown in Figure 12. This is similar to the three-party scenario described in figures 6A-6Q except for the fact that now there is more parties involved. Note participants 3,4,5,6 ... *n*-2 that have been arranged in series 1180. Each of the participants prepares his own message, incorporates it with the message he receives from a prior participant, if any, appends a digital signature with the message, and then sends it to the next participant in the line. The combined message is eventually sent to the SP and the SP forms the response message accordingly and sends it back through the same path the original request message has traveled.

Figure 13 shows elements arranged in a hierarchical organization scheme, where each element, $X_{1,1}$ to $X_{1,n}$ (n= 1, 2, 3, ...) 1200, is a participant of the transaction and not a message router, and each element, $X_{j,k}$ (j = 2, 3, 4, ...; k = 1, 2, 3, ...m; m is a variable of type n; m may be a different value for different levels of a hierarchy) 1210, can either be a participant or a router. The upward pointing bold arrow represents sending a request message 1220. The downward pointing arrow represents sending a response message 1230.

Each participant collects messages from a number of participants he is responsible for and, after combining the messages with his own and forming a new message, sends the new message to the next level. A hierarchical organization scheme may include only one participant to as many as is required (The most regressive case of the hierarchical scheme is one participant and one service provider). Eventually, at the last element before the service provider, $X_{\sigma,1}$ where σ is of type n, all messages are combined into one message 1240, which is then sent to the SP 60. Again, the SP forms the response message and sends it back through the same route.

In the case when the SP is not directing the transaction, the members are conducting the transaction among themselves using the session key generated by the SP. A transaction can occur between two or more members. When there are more than two members involved in the transaction, the messages can flow from member to member in any order. A member sends a transaction request message and receives a transaction response message. A member does not necessarily have to receive a transaction response message from the same member that he sent the transaction request message. For example, three members in a transaction can be organized in a ring and send messages around the ring. A first member can send a transaction request message to a second member who in turn sends a transaction request message and a transaction response message to third member. The third member sends a transaction request message and a transaction response message to the first member, and the first member sends a transaction response message to a second member. A member receiving a transaction request message creates a transaction response message, which eventually will be sent to the member who sent the transaction request message.

During the key exchange phase, the SP obtains the public keys of all the transaction participating members. The SP sends to each participating member, the other members' public keys prior to the participating members conducting a transaction among them. The transaction request messages and the transaction response message include plain text, if any, a cryptogram, and a digital signature of the sending party.

In the case when the SP needs to act as the surrogate-certificate for the EC and/or the merchant in order to deal with a certificate-based external system, the SP shields the EC and/or the merchant from the operation of the external interface. The SP only returns to the EC and/or the merchant, the information needed to complete the transaction with the EC and/or the merchant.

While there have been described herein what are considered to be preferred and exemplary embodiments of the present invention, other modifications of the invention shall be apparent to those with ordinary skill in the art. Therefore, it is desired to be secured in the appended claims all such modifications and extensions as fall with within the true spirit and scope of the invention. The invention is to be construed as including all embodiments thereof that fall within the scope of the appended claims and the invention should only be limited by the appended claims below. In addition, one with ordinary skill in the art will readily appreciate that other applications may be substituted for those set forth herein without departing from the spirit and scope of the present invention.

What is claimed:

1. A system for electronic transactions comprising:

an electronic card having,

a cryptographic service for encryption and decryption,

a data area for storing cardholder information, and

a data area for storing service provider information;

a service provider member terminal responsive to activation of the electronic card; and

a service provider terminal in communication with the service provider member terminal, the service provider terminal decrypting communication from the service provider member terminal and encrypting communication to the service provider member terminal, the service provider member terminal encrypting communication to the service provider terminal and decrypting communication from the service provider terminal.

2. The system of claim 1 wherein the electronic card is a physical card.

3. The system of claim 1 further comprising software having the electronic card.

4. The system of claim 1 wherein the electronic card further comprises a card operating system for loading and updating cardholder information, changing access conditions, and managing the service provider data area.

5. The system of claim 1 wherein the electronic card performs external communication read/write operations, and communication protocol handling.

6. The system of claim 1 wherein the electronic card further comprises software to manage the electronic card.

7. The system of claim 1 wherein the electronic card further comprises application software.

8. The system of claim 1 wherein the electronic card further comprises applets.

9. The system of claim 1 further comprising an external system wherein the service provider terminal communicates with the external system.

10. The system of claim 1 wherein the data area for storing service provider information includes at least one service provider record, each service provider record comprising:

a name field indicating the service provider;

at least one key value;

a key-type indication indicating the type of the key value; and

an account information field containing information unique to each service provider.

11. The system of claim 10 wherein the service provider record further comprises an instrument-type indication indicating the type of instrument a service provider supports.

12. The system of claim 10 wherein the service provider record further comprises an access condition, which a user must satisfy to gain access to the service provider information.

13. A method of conducting an electronic transaction using an electronic card comprising:

formatting a key exchange request message at a member;

sending the key exchange request message from the member to a service provider;

generating a session key at the service provider;

formatting a key exchange response message including the session key at the service provider;

sending the key exchange response message from the service provider to the member; and

using the session key to conduct a transaction.

14. A method of conducting an electronic transaction using an electronic card comprising:

formatting a key exchange request message at a member, the key exchange request message has a member challenge for the service provider;

sending the key exchange request message from the member to a service provider;

generating a session key at the service provider;

formatting a key exchange response message including the session key at the service provider, the key exchange response message has a response for the member challenge and a service provider challenge for the member and sending it to the member;

formatting by the member a response for the service provider challenge and sending it to the service provider; and

using the session key to conduct a transaction.

15. The method of claim 13 or 14 wherein the step of using the session key to conduct a transaction comprises the steps of:

formatting by a member a transaction request message using the session key, the transaction request message including a digital signature of the member, and sending the transaction request message to the service provider; and

formatting at the service provider, a transaction response message for the member using the session key, the transaction response including a digital signature of the service provider, and sending the transaction response message to the member.

16. The method of claim 15 wherein the member encrypts, using the session key assigned to him by the service provider, his account information, the transaction amount and sensitive transaction data in his transaction request message, the sensitive transaction data being information that is accessible only to the service provider.

17. The method of claim 15 wherein the member includes plain text in his transaction request message.

18. The method of claim 15 wherein the member includes the transaction identification assigned to him by the service provider, in his transaction request message.

19. The method of claim 15 wherein the member includes a response to a service provider challenge in his transaction request message.

20. The method of claim 15 wherein the service provider encrypts the response data for the member using member's session key and include the cryptogram as part of its transaction response message to the member.

21. The method of claim 15 wherein the service provider includes plain text in its transaction response message to the member.

22. The method of claim 15 wherein the service provider includes member's transaction identification in his transaction response message to the member.

23 The method of claim 15 further comprises the steps of:
formatting at the member, using the session key, a transaction acknowledgment message, including a digital signature of the sending member, and sending the transaction acknowledgment message to the service provider.

24. The method of claim 15 wherein the member encrypts, using the session key assigned to him by the service provider, his acknowledgment data in his acknowledgment message.

25. The method of claim 15 wherein the member includes plain text in his acknowledgment message.

26. The method of claim 15 wherein the member includes the transaction

identification assigned to him by the service provider, in his acknowledgment message.

27. The method of claim 15 wherein the member chooses to encrypt sensitive information in the transaction acknowledgment message, the sensitive information being information that is accessible only to the service provider.

28. The method of claim 13 or 14 of conducting a key exchange comprising:

generating a member challenge by the member;

encrypting by the member the member challenge using the service provider's public key and generating a first cryptogram;

formatting by the member a key exchange request message including the first cryptogram and member's public key;

singing digitally by the member the key exchange request message;

sending the digitally signed key exchange request message to the service provider;

generating by the service provider a service provider challenge;

generating by the service provider a session key;

encrypting by the service provider the service provider challenge and the session key using the member's public key and generating a second cryptogram;

formatting by the service provider a key exchange response message including the second cryptogram and the response to member challenge;

signing digitally by the service provider the key exchange response message;

sending digitally signed key exchange response message to the member;

encrypting by the member the member response for the service provider challenge using the session key and generating a third cryptogram;

attaching the third cryptogram to the next message going from the member to the service provider;

signing digitally by the member the next message going from the member to the service provider; and

sending the next message going from the member to the service provider to the service provider.

29. The method of claim 28 wherein the member uses different pairs of private and public keys for different transactions in the messages to communicate with the service provider.

30. The method of claim 28 wherein the key exchange request message and key exchange response message contain plaintext

31. The method of claim 28 wherein the member chooses to encrypt his own public key using the service provider's public key in the key exchange request message.

32. The method of claim 28 wherein the member and service provider chooses to encrypt sensitive information in the key exchange request message and the key exchange response message, the sensitive information being information that is accessible only to the service provider and the corresponding member.

33. The method of claim 28 wherein the service provider encrypts the response to the member challenge as part of the second cryptogram.

34. The method of claim 28 wherein the service provider encrypts transaction identification as part of the second cryptogram.

35. The method of claim 28 wherein the service provider includes a transaction identification as part of the plain text in the key exchange response message.

36. The method of claim 34 wherein the member uses the transaction identification in the next message going from the member to the service provider.

37. The method of claim 35 wherein the member uses the transaction identification in the next message going from the member to the service provider.

38. The method of claim 13 or 14 of conducting a key exchange between two members and a service provider comprises the steps of:

sending a key exchange request message from the first member to a second member;

combining at the second member, a second member key exchange request message with the first member's key exchange request message and sending the combined key exchange request message, signed by the second member, to a service provider;

formatting a key exchange response message at the service provider including the session key for the first member, signing the response message, formatting a key exchange response message including the session key for the second member, combining the key exchange response messages into a combined key exchange response message, signing the combined key exchange response message, and sending the combined key exchange response message to the second member; and

separating at the second member, the key exchange response message for the second member from the key exchange response message for the first member, and forwarding the key exchange response message for the first member to the first member.

39. A method of claim 13 or 14 wherein the step of conducting a transaction between two members and a service provider comprising:

formatting by a first member, using the first member's session key, a transaction request message, the transaction request message including a digital signature of the first member, and sending the transaction request message to a second member; and

formatting by the second member, using the second member's session key, a transaction request message;

combining by the second member, the second member transaction request message with the first member transaction request message, the combined transaction request message including a digital signature of the second member, and sending the combined transaction request message to a service provider;

formatting by the service provider, using the first member's session key, a transaction response message for the first member, including a digital signature of the service provider;

formatting by the service provider, using the second member's session key, a transaction response message for the second member;

combining the transaction response message for the first member with the transaction response message for the second member and forming a combined transaction response message, the combined transaction response message including a digital signature of the service provider;

sending the combined transaction response message to the second member;

separating at the second member, the transaction response message for the first member from the transaction response message for the second member;

forwarding by the second member the transaction response message for the first member to the first member.

40. The method of claim 39 further comprises the steps of:

formatting at a first member, using the first member's session key, an acknowledgment message, the acknowledgment message including a digital signature of the first member, and sending the acknowledgment message to a second member; and

formatting at the second member, using the second member's session key, an acknowledgment message, combining the second member acknowledgment message with the first member acknowledgment message and forming a combined acknowledgment message, the combined acknowledgment message including a digital signature of' the second member, and sending the combined acknowledgment message to the service provider.

41. The method of claim 13 or 14 of conducting a key exchange between multiple members and a service provider arranged in series comprising the steps of:

formatting a key exchange request message at a first member;

sending the key exchange request message from the first member to a second member where the second member is a message router or participating member;

sending a key exchange request message from the second member to a next member, if the second member is a message router;

combining the second member's key exchange request message with the first member's key exchange request message and sending the combined key exchange message to the next member if the second member is a participating member;

sending the combined key exchange request message to the next member if the current member is a message router;

combining a current member's key exchange request message with a previous member's key exchange request message and sending the combined key exchange request message to a next member, if the current member is a participating member;

sending the combined key exchange request to a service provider if the current member is the last participating member or message router;

generating at the service provider different session keys for different participating members;

formatting, by the service provider, into one message, a key exchange response message including the different session keys for different participating members and sending the combined key exchange response message in reverse order of the path for sending the combined key exchange request to the service provider; and

separating, by every participating member, the key exchange response message for itself from the key exchange response messages for the other participating members, and forwarding the remaining key exchange response messages to the other participating members in reverse order of the path for sending the combined key exchange request to the service provider, until the first member receives its key exchange response message.

42. The method of claim 13 or 14 of conducting a transaction using session keys between multiple members and a service provider arranged in series comprising the steps of:

formatting a transaction request message at a first member;

sending a transaction request message from the first member to a second member where the second member is a message router or participating member;

sending the transaction request message from the second member to a next member, if the second member is a message router;

combining the second member's transaction request message with the first member's transaction request message and sending the combined transaction message to the next member if the second member is a participating member;

sending the combined transaction request message to the next member if the current member is a message router;

combining a current member's transaction request message with a previous member's transaction request message and sending the combined transaction request message to a next member, if the current member is a participating member;

sending the combined transaction request to a service provider if the current member is the last participating member or message router;

formatting, by the service provider, into one message, a transaction response message and sending the combined transaction response message in reverse order of the path for sending the combined transaction request to the service provider; and

separating, by every participating member, the transaction response for itself from the transaction response for the other participating members, and forwarding the remaining transaction response to the other participating members in reverse order of the path for sending the combined transaction request message to the service provider, until the first member receives its transaction response.

43. The method of claim 13 or 14 of conducting a key exchange between multiple members and a service provider arranged in a hierarchical organization comprising the steps of:

formatting a key exchange request message at a first member;

sending the key exchange request message from the first member to a next member Xj,k (j=2,3,4.....; k=1,2,3.....m; m is a variable of type n; n=1,2,3...; m can be different values of j) if the second member is a message router;

combining a second member's key exchange request message with the first member's key exchange request message and sending the combined key exchange request message to a next member Xj,k if the second member is a participating member;

sending the combined key exchange request message to the next member Xj,k if a current member Xj,k is a message router;

combining a current member Xj,k's key exchange request message with a previous member's key exchange request message and sending the combined key exchange request message to the next member Xj,k, if the current member Xj,k, is a participating member;

sending the combined key exchange request to a service provider if the current member is the last participating member;

generating at the service provider different session keys for different participating members;

formatting, by the service provider, into one message, a key exchange response message including the different session keys for different participating member and sending the combined key exchange response message in reverse order of the path for sending the combined key exchange request to the service provider; and

separating, by every participating, the key exchange response message for itself from the key exchange response messages for the other participating members in reverse order of the path for sending the key exchange request to the service provider, until the first member receives its key exchange response message.

44. The method of claim 13 or 14 of conducting a transaction using session keys between multiple members and a service provider arranged in a hierarchical organization comprising the steps of:

formatting a transaction request message at a first member;

sending the transaction request message from the first member to a next member Xj,k (j = 2, 3, 4, . . . ; k = 1, 2, 3, . . . m; m is a variable of type n; n= 1, 2, 3, . . . ; m can be different values of j) if the second member is a message router;

combining a second member's transaction request message with the first member's transaction request message and sending the combined transaction request message to a next member Xj,k if the second member is a participating member;

sending the combined transaction request message to the next member Xj,k if a current member Xj,k is a message router;

combining a current member Xj,k's transaction request message with a previous member's transaction request message and sending the combined transaction request message to the next party Xj,k if the current member Xj,k a participating member;

sending the combined transaction request to a service provider if the current member is the last participating member or message router;

formatting, by the service provider, into one message, a transaction response message for each participating member and sending the combined transaction response message in reverse order of the path for each participating member and sending the combined transaction request to the service provider; and

separating, by every participating, transaction response message for itself from the transaction response messages for the other participating members in reverse order of the path for sending the transaction request to the service provider, until the first member receives its transaction response message.

45. The method of claim 13 or 14 of conducting a key exchange between two members and a service provider comprises the steps of:

sending a key exchange request message from the first member to a second member;

combining at the second member, a second member key exchange request message with the first member's key exchange request message and sending the combined key exchange request message, signed by the second member, to a service provider;

generating at the service provider a session key used for both the first member and the second member;

formatting a key exchange response message at the service provider including the session key for the first member, signing the response message, formatting a key exchange response message including the session key for the second member, combining the key exchange response messages into a combined key exchange response message, signing the combined key exchange response message, and sending the combined key exchange response message to the second member; and

separating at the second member, the key exchange response message for the second member from the key exchange response message for the first member, and forwarding the key exchange response message for the first member to the first member.

46. The method of claim 13 or 14 of conducting a key exchange between multiple members and a service provider arranged in series comprising the steps of:

formatting a key exchange request message at a first member;

sending the key exchange request message from the first member to a second member where the second member is a message router or participating member;

sending a key exchange request message from the second member to a next member, if the second member is a message router;

combining the second member's key exchange request message with the first member's key exchange request message and sending the combined key exchange message to the next member if the second member is a participating member;

sending the combined key exchange request message to the next member if the current member is a message router;

combining a current member's key exchange request message with a previous member's key exchange request message and sending the combined key exchange request message to a next member, if the current member is a participating member;

sending the combined key exchange request to a service provider if the current member is the last participating member or message router;

generating at the service provider a session key for the participating members;

formatting, by the service provider, into one message, a key exchange response message including the session key for the participating members and sending the combined key exchange response message in reverse order of the path for sending the combined key exchange request to the service provider; and

separating, by every participating member, the key exchange response message for itself from the key exchange response messages for the other participating members, and forwarding the remaining key exchange response messages to the other participating members in reverse order of the path for sending the combined key exchange request to the service provider, until the first member receives its key exchange response message.

47. The method of claim 13 or 14 of conducting a key exchange between multiple members and a service provider arranged in a hierarchical organization comprising the steps of:

formatting a key exchange request message at a first member;

sending the key exchange request message from the first member to a next member Xj,k (j=2,3,4.....; k=1,2,3.....m; m is a variable of type n; n=1,2,3...; m can be different values of j) if the second member is a message router;

combining a second member's key exchange request message with the first member's key exchange request message and sending the combined key exchange request message to a next member Xj,k if the second member is a participating member;

sending the combined key exchange request message to the next member Xj,k if a current member Xj,k is a message router;

combining a current member Xj,k's key exchange request message with a previous member's key exchange request message and sending the combined key exchange request message to the next member Xj,k, if the current member Xj,k, is a participating member; sending the combined key exchange request to a service provider if the current member is the last participating member or message router;

generating at the service provider a session key for the participating members;

formatting, by the service provider, into one message, a key exchange response message including the session key for the participating member and sending the combined key exchange response message in reverse order of the path for sending the combined key exchange request to the service provider; and

separating, by every participating, the key exchange response message for itself from the key exchange response messages for the other participating members in reverse order of the path for sending the key exchange request to the service provider, until the first member receives its key exchange response message.

48. The method of claim 38 wherein the service provider provides each member involved in a transaction with other member's public keys.

49. The method of claim 41 wherein the service provider provides each member involved in a transaction with other member's public keys.

50. The method of claim 43 wherein the service provider provides each member involved in a transaction with other member's public keys.

51. The method of claim 45 wherein the service provider provides each member

involved in a transaction with other member's public keys.

52. The method of claim 46 wherein the service provider provides each member involved in a transaction with other member's public keys.

53. The method of claim 47 wherein the service provider provides each member involved in a transaction with other member's public keys.

A CRYPTOGRAPHIC SYSTEM AND METHOD FOR ELECTRONIC TRANSACTIONS

ABSTRACT OF THE DISCLOSURE

An electronic transaction system, which facilitates secure electronic transactions among multiple parties including cardholders, merchants, and service providers (SP). The system involves electronic cards, commonly known as smart cards, and their equivalent computer software package. The card mimics a real wallet and contains commonly seen financial or non-financial instruments such as a credit card, checkbook, or driver license. A transaction is protected by a hybrid key cryptographic system and is normally carried out on a public network such as the Internet. Digital signatures and challenges – responses are used to ensure integrity and authenticity. The card utilizes secret keys such as session keys assigned by service providers (SPs) to ensure privacy for each transaction. The SP is solely responsible for validating each participant's sensitive information and assigning session keys. The system does not seek to establish a trust relationship between two participants of a transaction. The only trust relationship needed in a transaction is the one that exists between individual participants and the SP. The trust relationship with a participant is established when the SP has received and validated certain established account information from that particular participant. To start a transaction with a selected SP, a participant must have the public key of the intended SP. Since the public key is openly available, its availability can be easily established by the cardholder. The SP also acts as a gateway for the participants when a transaction involves interaction with external systems.

AH/ah
#184297v2

FIG. 1

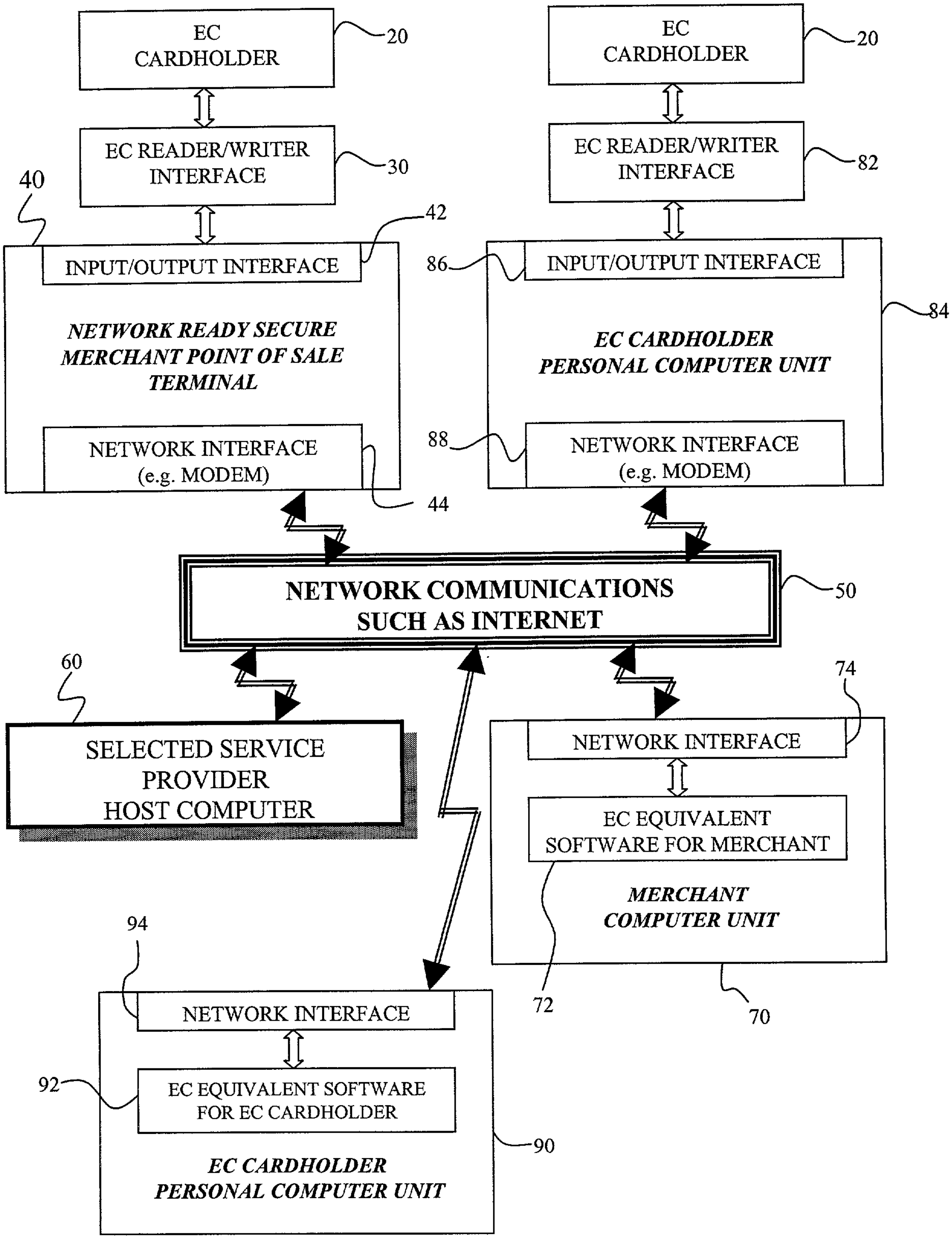

EC CARDHOLDER
20
EC READER/WRITER INTERFACE
30
40
42
INPUT/OUTPUT INTERFACE
NETWORK READY SECURE MERCHANT POINT OF SALE TERMINAL
NETWORK INTERFACE (e.g. MODEM)
44
EC CARDHOLDER
20
EC READER/WRITER INTERFACE
82
86
INPUT/OUTPUT INTERFACE
84
EC CARDHOLDER PERSONAL COMPUTER UNIT
88
NETWORK INTERFACE (e.g. MODEM)
NETWORK COMMUNICATIONS SUCH AS INTERNET
50
60
SELECTED SERVICE PROVIDER HOST COMPUTER
74
NETWORK INTERFACE
EC EQUIVALENT SOFTWARE FOR MERCHANT
MERCHANT COMPUTER UNIT
72
70
94
NETWORK INTERFACE
92
EC EQUIVALENT SOFTWARE FOR EC CARDHOLDER
90
EC CARDHOLDER PERSONAL COMPUTER UNIT

FIG. 2

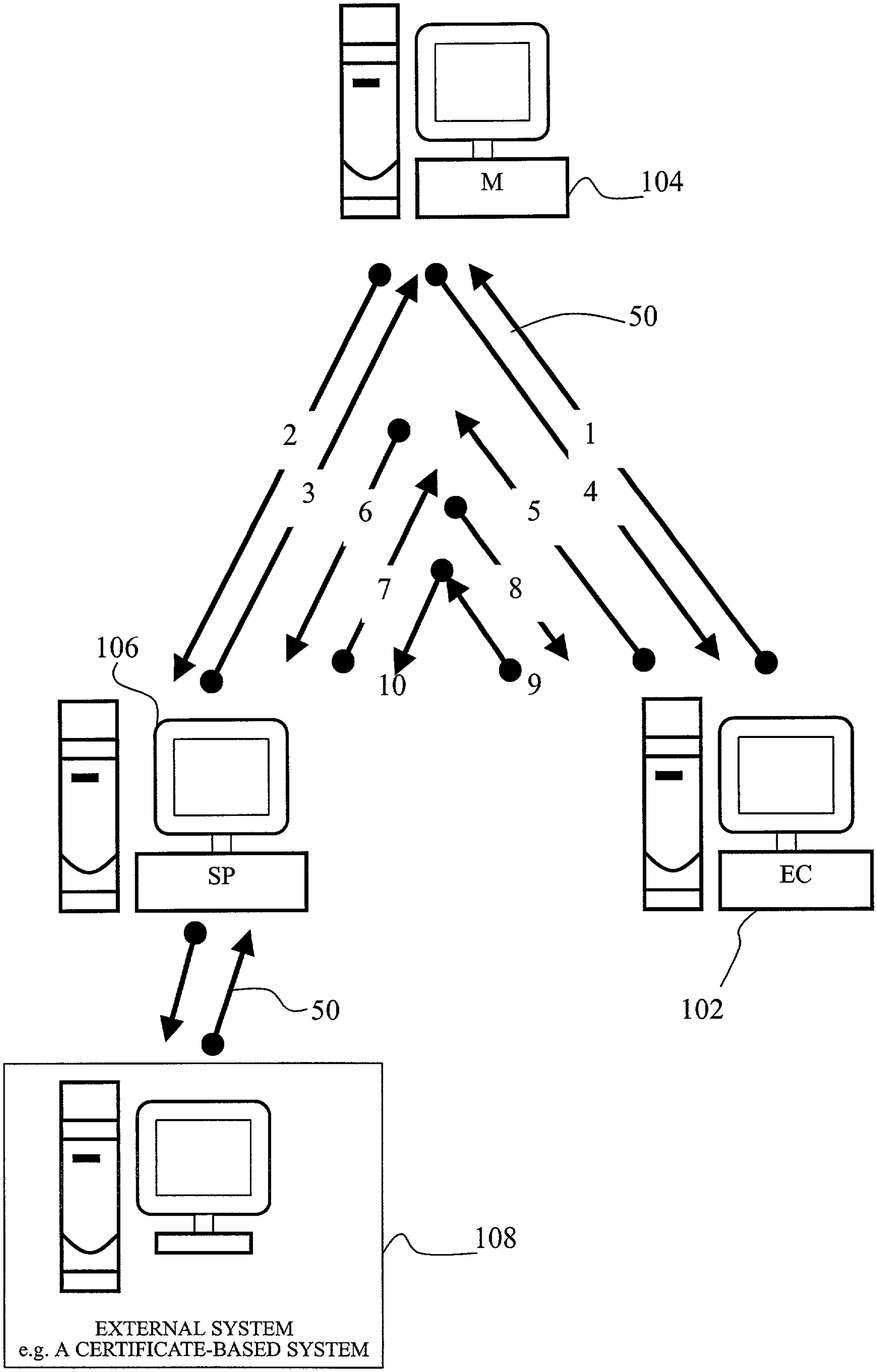
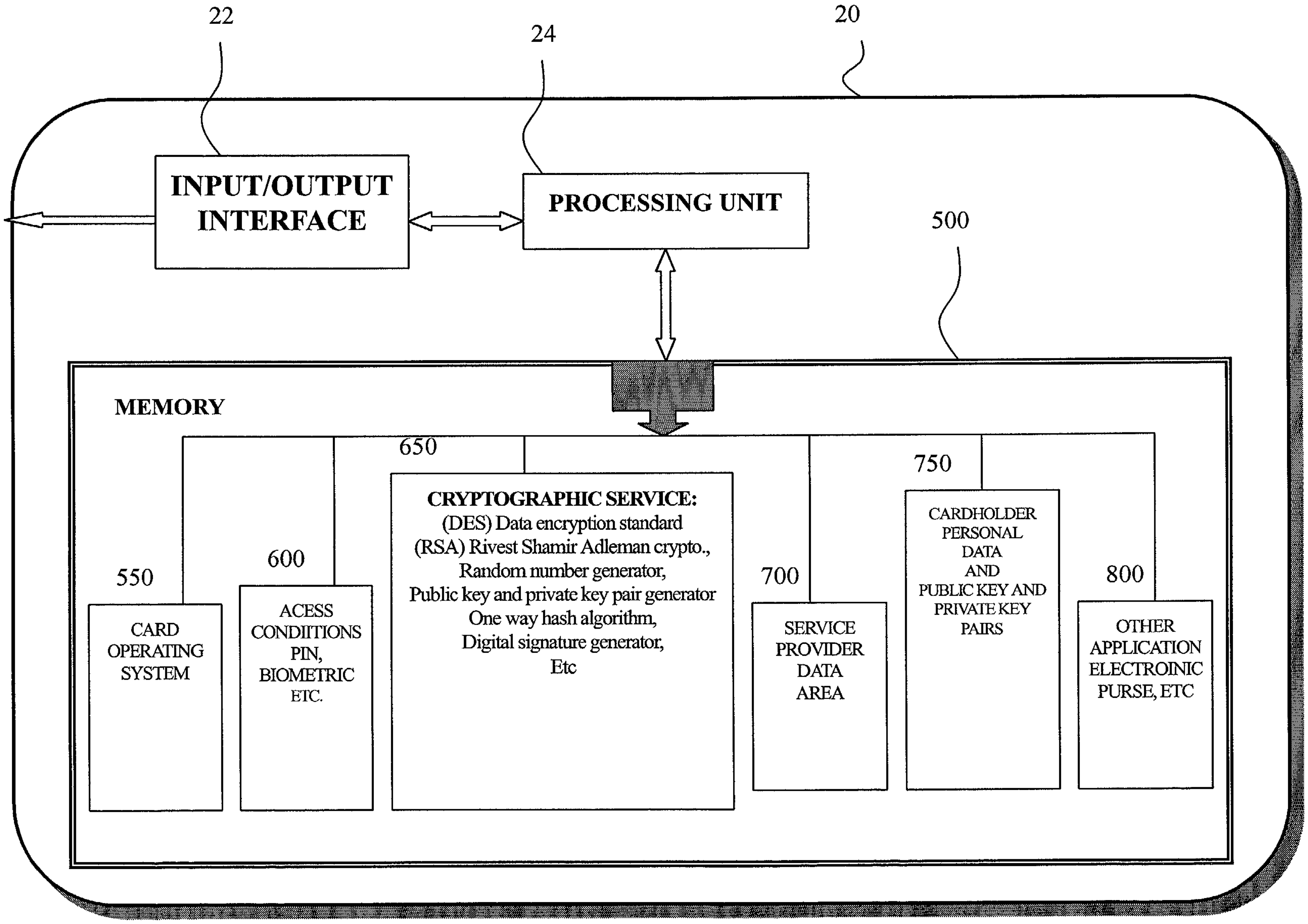

M
104
50
2
1
3
6
5
4
7
8
106
10
9
SP
EC
50
102
108
EXTERNAL SYSTEM
e.g. A CERTIFICATE-BASED SYSTEM

FIG. 3


22
24
20
INPUT/OUTPUT INTERFACE
PROCESSING UNIT
500
MEMORY
650
750
550
600
700
800
CARD OPERATING SYSTEM
ACESS CONDITIONS PIN, BIOMETRIC ETC.
CRYPTOGRAPHIC SERVICE:
(DES) Data encryption standard
(RSA) Rivest Shamir Adleman crypto.,
Random number generator,
Public key and private key pair generator
One way hash algorithm,
Digital signature generator,
Etc
SERVICE PROVIDER DATA AREA
CARDHOLDER PERSONAL DATA AND PUBLIC KEY AND PRIVATE KEY PAIRS
OTHER APPLICATION ELECTROINIC PURSE, ETC

ELECTRONIC CARD

FIG. 4

700

SERVICE PROVIDERS' DATA AREA (SPDA)

702	704	706	708	710	712	714
NAME	KEY TYPE	KEY VALUE	ACCOUNT INFORMATION (Number, expiration date, etc.)	CARD TYPE	PIN (optional)	Miscellaneous Data
				CREDIT CARD		
				DEBIT CARD		
				ATM CARD		
				MEMBER CARD		
				LOYALTY CARD		
				etc.		

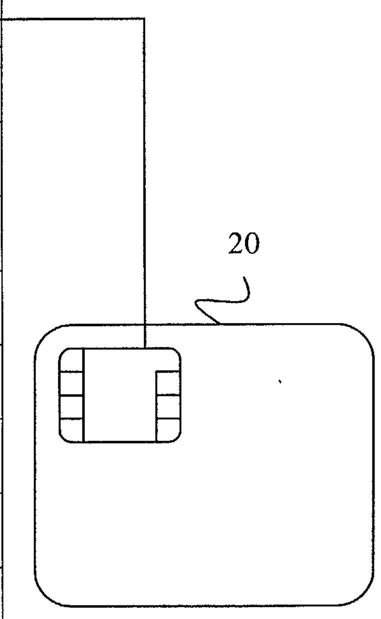


FIG. 5

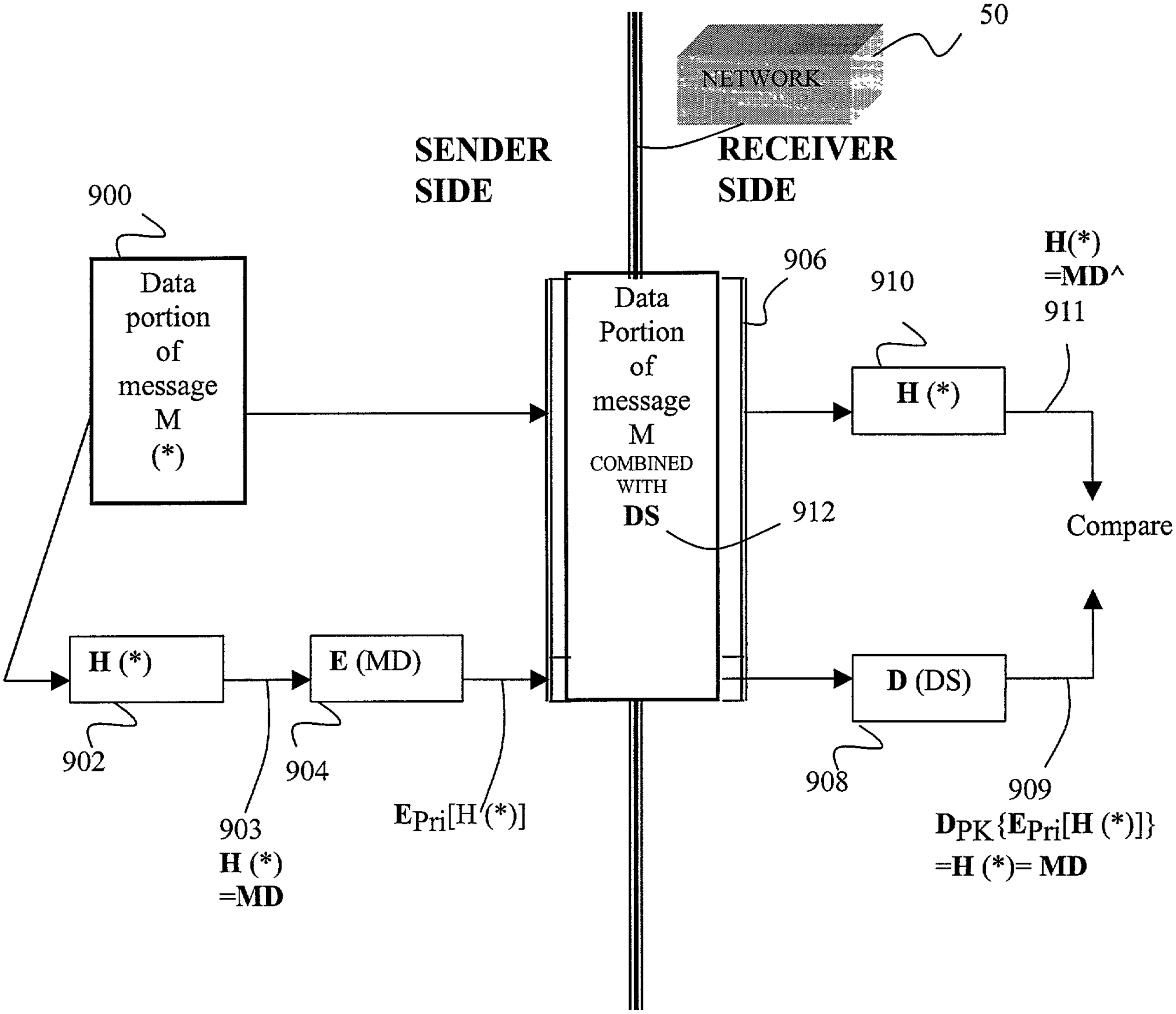

50
NETWORK
SENDER SIDE
RECEIVER SIDE
900
Data portion of message M (*)
906
Data Portion of message M COMBINED WITH DS
912
910
H (*)
H(*) =MD^
911
Compare
H (*)
902
903
H (*) =MD
E (MD)
904
EPri[H (*)]
D (DS)
908
909
DPK{EPri[H (*)]}
=H (*)= MD

FIG. 6A

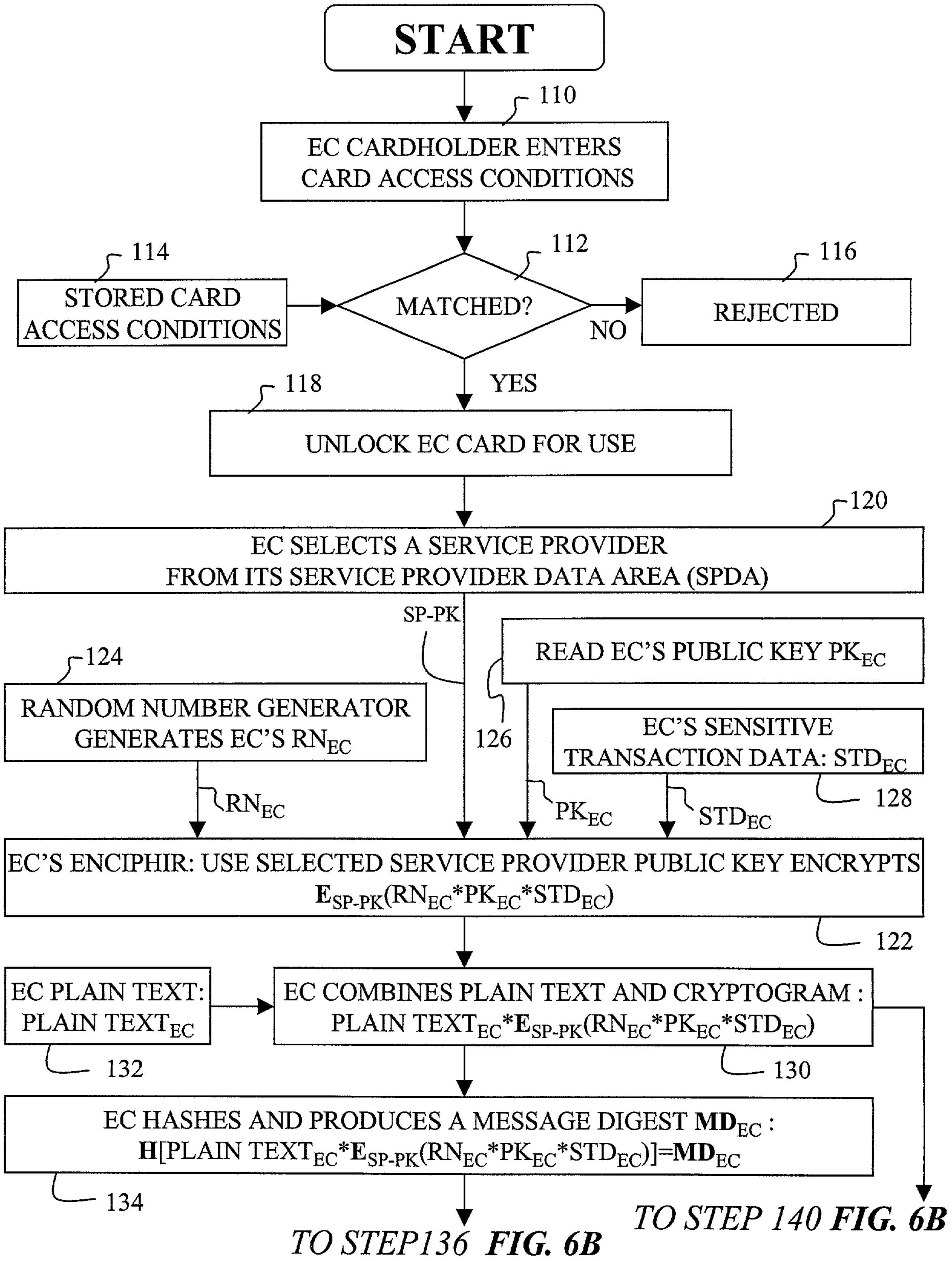

START
110
EC CARDHOLDER ENTERS CARD ACCESS CONDITIONS
114
STORED CARD ACCESS CONDITIONS
112
MATCHED?
NO
116
REJECTED
YES
118
UNLOCK EC CARD FOR USE
120
EC SELECTS A SERVICE PROVIDER FROM ITS SERVICE PROVIDER DATA AREA (SPDA)
SP-PK
READ EC'S PUBLIC KEY PK_{EC}
124
RANDOM NUMBER GENERATOR GENERATES EC'S RN_{EC}
126
EC'S SENSITIVE TRANSACTION DATA: STD_{EC}
128
RN_{EC}
PK_{EC}
STD_{EC}
EC'S ENCIPHIR: USE SELECTED SERVICE PROVIDER PUBLIC KEY ENCRYPTS $E_{SP\text{-}PK}(RN_{EC}*PK_{EC}*STD_{EC})$
122
EC PLAIN TEXT: PLAIN $TEXT_{EC}$
EC COMBINES PLAIN TEXT AND CRYPTOGRAM : PLAIN $TEXT_{EC}*\mathbf{E}_{SP\text{-}PK}(RN_{EC}*PK_{EC}*STD_{EC})$
132
130
EC HASHES AND PRODUCES A MESSAGE DIGEST $\mathbf{MD}_{EC}$:
$\mathbf{H}[\text{PLAIN } TEXT_{EC}*\mathbf{E}_{SP\text{-}PK}(RN_{EC}*PK_{EC}*STD_{EC})]=\mathbf{MD}_{EC}$
134
TO STEP 140 FIG. 6B
TO STEP136 FIG. 6B

FIG. 6B

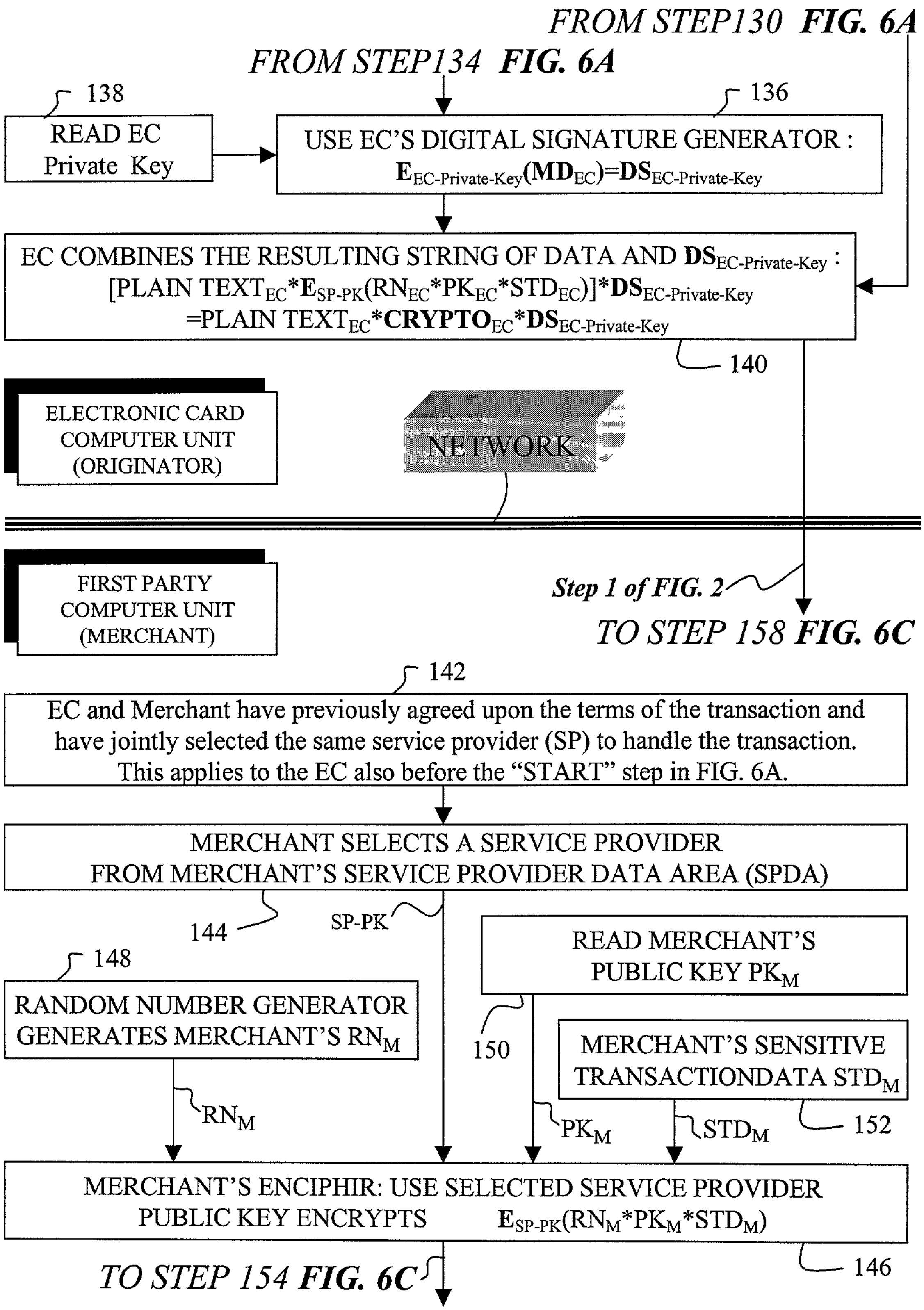

FROM STEP130 FIG. 6A
FROM STEP134 FIG. 6A
138
READ EC Private Key
136
USE EC'S DIGITAL SIGNATURE GENERATOR : $\mathbf{E}_{\text{EC-Private-Key}}(\mathbf{MD}_{\text{EC}})=\mathbf{DS}_{\text{EC-Private-Key}}$
EC COMBINES THE RESULTING STRING OF DATA AND $\mathbf{DS}_{\text{EC-Private-Key}}$:
$[\text{PLAIN TEXT}_{\text{EC}}*\mathbf{E}_{\text{SP-PK}}(\text{RN}_{\text{EC}}*\text{PK}_{\text{EC}}*\text{STD}_{\text{EC}})]*\mathbf{DS}_{\text{EC-Private-Key}}$
$=\text{PLAIN TEXT}_{\text{EC}}*\mathbf{CRYPTO}_{\text{EC}}*\mathbf{DS}_{\text{EC-Private-Key}}$
140
ELECTRONIC CARD COMPUTER UNIT (ORIGINATOR)
NETWORK
FIRST PARTY COMPUTER UNIT (MERCHANT)
Step 1 of FIG. 2
TO STEP 158 FIG. 6C
142
EC and Merchant have previously agreed upon the terms of the transaction and have jointly selected the same service provider (SP) to handle the transaction. This applies to the EC also before the "START" step in FIG. 6A.
MERCHANT SELECTS A SERVICE PROVIDER FROM MERCHANT'S SERVICE PROVIDER DATA AREA (SPDA)
144
SP-PK
148
RANDOM NUMBER GENERATOR GENERATES MERCHANT'S RN_{M}
READ MERCHANT'S PUBLIC KEY PK_{M}
150
MERCHANT'S SENSITIVE TRANSACTIONDATA STD_{M}
RN_{M}
PK_{M}
STD_{M}
152
MERCHANT'S ENCIPHIR: USE SELECTED SERVICE PROVIDER PUBLIC KEY ENCRYPTS $\mathbf{E}_{\text{SP-PK}}(\text{RN}_{\text{M}}*\text{PK}_{\text{M}}*\text{STD}_{\text{M}})$
146
TO STEP 154 FIG. 6C

FIG. 6C

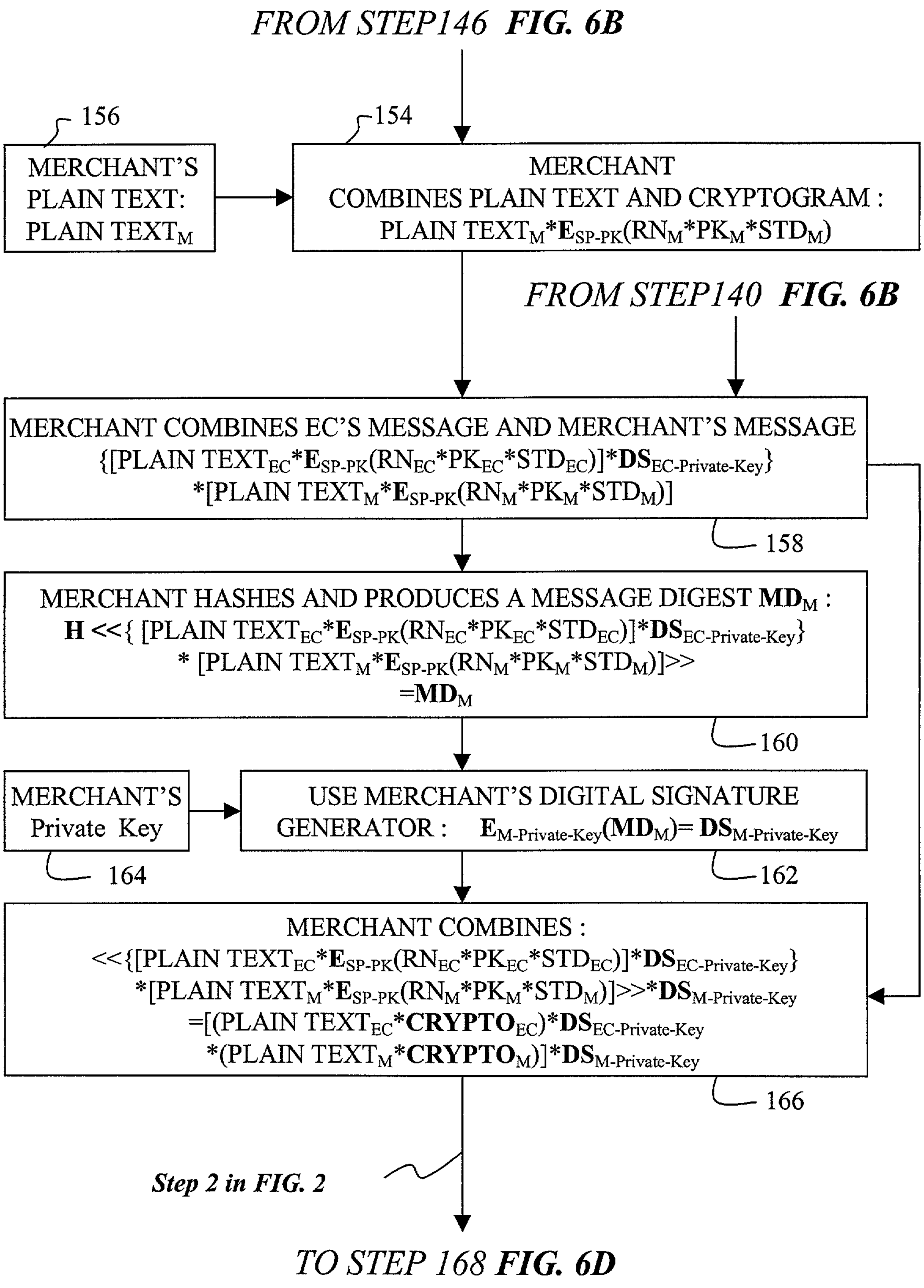
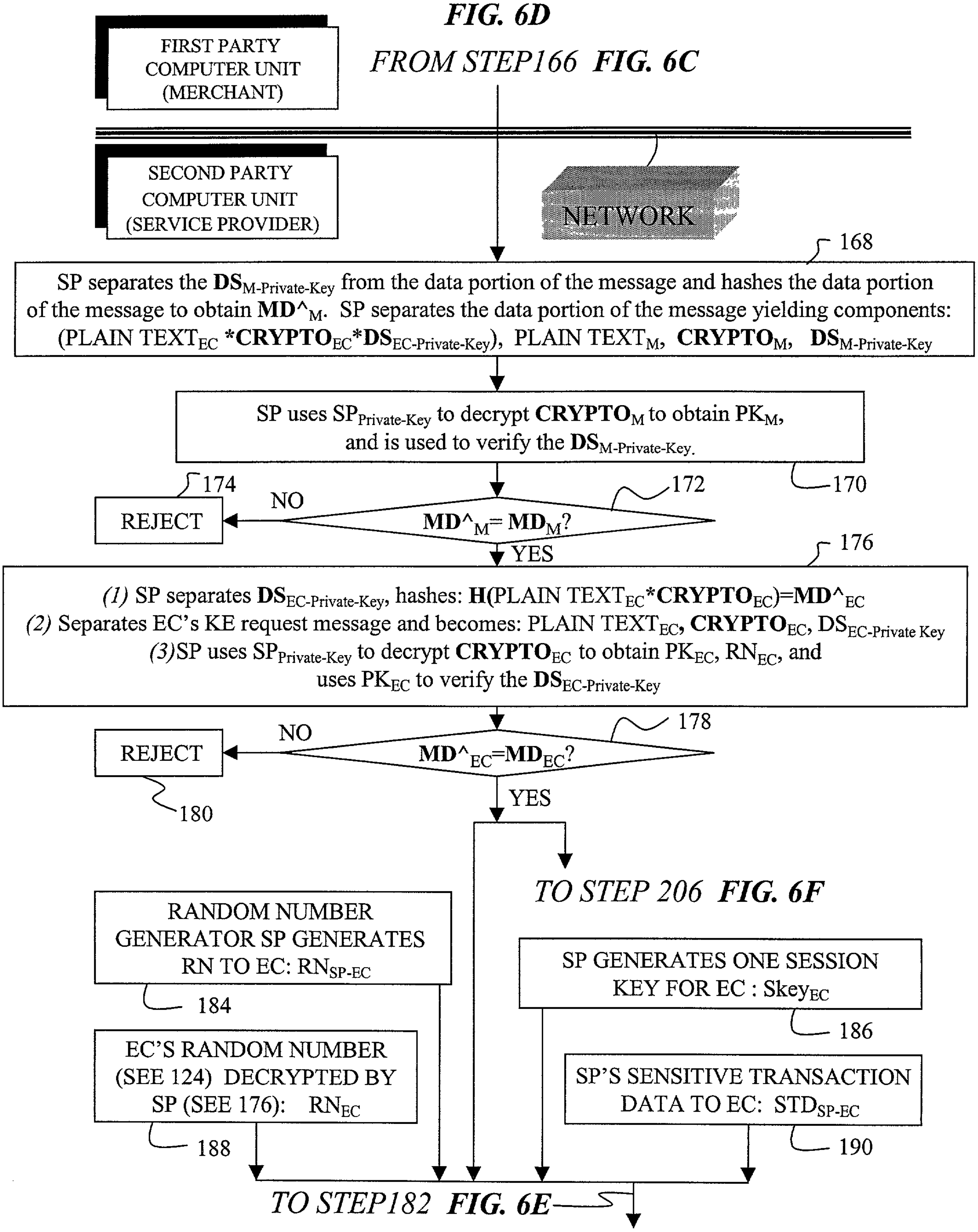

FROM STEP146 FIG. 6B
156
MERCHANT'S PLAIN TEXT: PLAIN TEXT_{M}
154
MERCHANT COMBINES PLAIN TEXT AND CRYPTOGRAM : PLAIN $\text{TEXT}_{M}*\mathbf{E}_{SP\text{-}PK}(RN_{M}*PK_{M}*STD_{M})$
FROM STEP140 FIG. 6B
MERCHANT COMBINES EC'S MESSAGE AND MERCHANT'S MESSAGE $\{[\text{PLAIN TEXT}_{EC}*\mathbf{E}_{SP\text{-}PK}(RN_{EC}*PK_{EC}*STD_{EC})]*\mathbf{DS}_{EC\text{-}Private\text{-}Key}\}$ $*[\text{PLAIN TEXT}_{M}*\mathbf{E}_{SP\text{-}PK}(RN_{M}*PK_{M}*STD_{M})]$
158
MERCHANT HASHES AND PRODUCES A MESSAGE DIGEST $\mathbf{MD}_{M}$: $\mathbf{H} \ll\{ [\text{PLAIN TEXT}_{EC}*\mathbf{E}_{SP\text{-}PK}(RN_{EC}*PK_{EC}*STD_{EC})]*\mathbf{DS}_{EC\text{-}Private\text{-}Key}\}$ $* [\text{PLAIN TEXT}_{M}*\mathbf{E}_{SP\text{-}PK}(RN_{M}*PK_{M}*STD_{M})]\gg$ $=\mathbf{MD}_{M}$
160
MERCHANT'S Private Key
164
USE MERCHANT'S DIGITAL SIGNATURE GENERATOR : $\mathbf{E}_{M\text{-}Private\text{-}Key}(\mathbf{MD}_{M})= \mathbf{DS}_{M\text{-}Private\text{-}Key}$
162
MERCHANT COMBINES : $\ll\{[\text{PLAIN TEXT}_{EC}*\mathbf{E}_{SP\text{-}PK}(RN_{EC}*PK_{EC}*STD_{EC})]*\mathbf{DS}_{EC\text{-}Private\text{-}Key}\}$ $*[\text{PLAIN TEXT}_{M}*\mathbf{E}_{SP\text{-}PK}(RN_{M}*PK_{M}*STD_{M})]\gg*\mathbf{DS}_{M\text{-}Private\text{-}Key}$ $=[(\text{PLAIN TEXT}_{EC}*\mathbf{CRYPTO}_{EC})*\mathbf{DS}_{EC\text{-}Private\text{-}Key}$ $*(\text{PLAIN TEXT}_{M}*\mathbf{CRYPTO}_{M})]*\mathbf{DS}_{M\text{-}Private\text{-}Key}$
166
Step 2 in FIG. 2
TO STEP 168 FIG. 6D

FIG. 6D



FROM STEP166 FIG. 6C
FIRST PARTY COMPUTER UNIT (MERCHANT)
SECOND PARTY COMPUTER UNIT (SERVICE PROVIDER)
NETWORK
168
SP separates the $\mathbf{DS}_{M\text{-}Private\text{-}Key}$ from the data portion of the message and hashes the data portion of the message to obtain $\mathbf{MD}^\wedge_M$. SP separates the data portion of the message yielding components: (PLAIN $TEXT_{EC}$ $*\mathbf{CRYPTO}_{EC}*\mathbf{DS}_{EC\text{-}Private\text{-}Key}$), PLAIN $TEXT_M$, $\mathbf{CRYPTO}_M$, $\mathbf{DS}_{M\text{-}Private\text{-}Key}$
SP uses $SP_{Private\text{-}Key}$ to decrypt $\mathbf{CRYPTO}_M$ to obtain PK_M, and is used to verify the $\mathbf{DS}_{M\text{-}Private\text{-}Key.}$
170
174
REJECT
NO
172
$\mathbf{MD}^\wedge_M = \mathbf{MD}_M$?
YES
176
(1) SP separates $\mathbf{DS}_{EC\text{-}Private\text{-}Key}$, hashes: $\mathbf{H}$(PLAIN $TEXT_{EC}$$*\mathbf{CRYPTO}_{EC}$)=$\mathbf{MD}^\wedge_{EC}$
(2) Separates EC's KE request message and becomes: PLAIN $TEXT_{EC}$, $\mathbf{CRYPTO}_{EC}$, $DS_{EC\text{-}Private\ Key}$
(3)SP uses $SP_{Private\text{-}Key}$ to decrypt $\mathbf{CRYPTO}_{EC}$ to obtain PK_{EC}, RN_{EC}, and uses PK_{EC} to verify the $\mathbf{DS}_{EC\text{-}Private\text{-}Key}$
REJECT
NO
178
$\mathbf{MD}^\wedge_{EC} = \mathbf{MD}_{EC}$?
180
YES
TO STEP 206 FIG. 6F
RANDOM NUMBER GENERATOR SP GENERATES RN TO EC: $RN_{SP\text{-}EC}$
184
SP GENERATES ONE SESSION KEY FOR EC : $Skey_{EC}$
186
EC'S RANDOM NUMBER (SEE 124) DECRYPTED BY SP (SEE 176): RN_{EC}
188
SP'S SENSITIVE TRANSACTION DATA TO EC: $STD_{SP\text{-}EC}$
190
TO STEP182 FIG. 6E

FIG. 6E

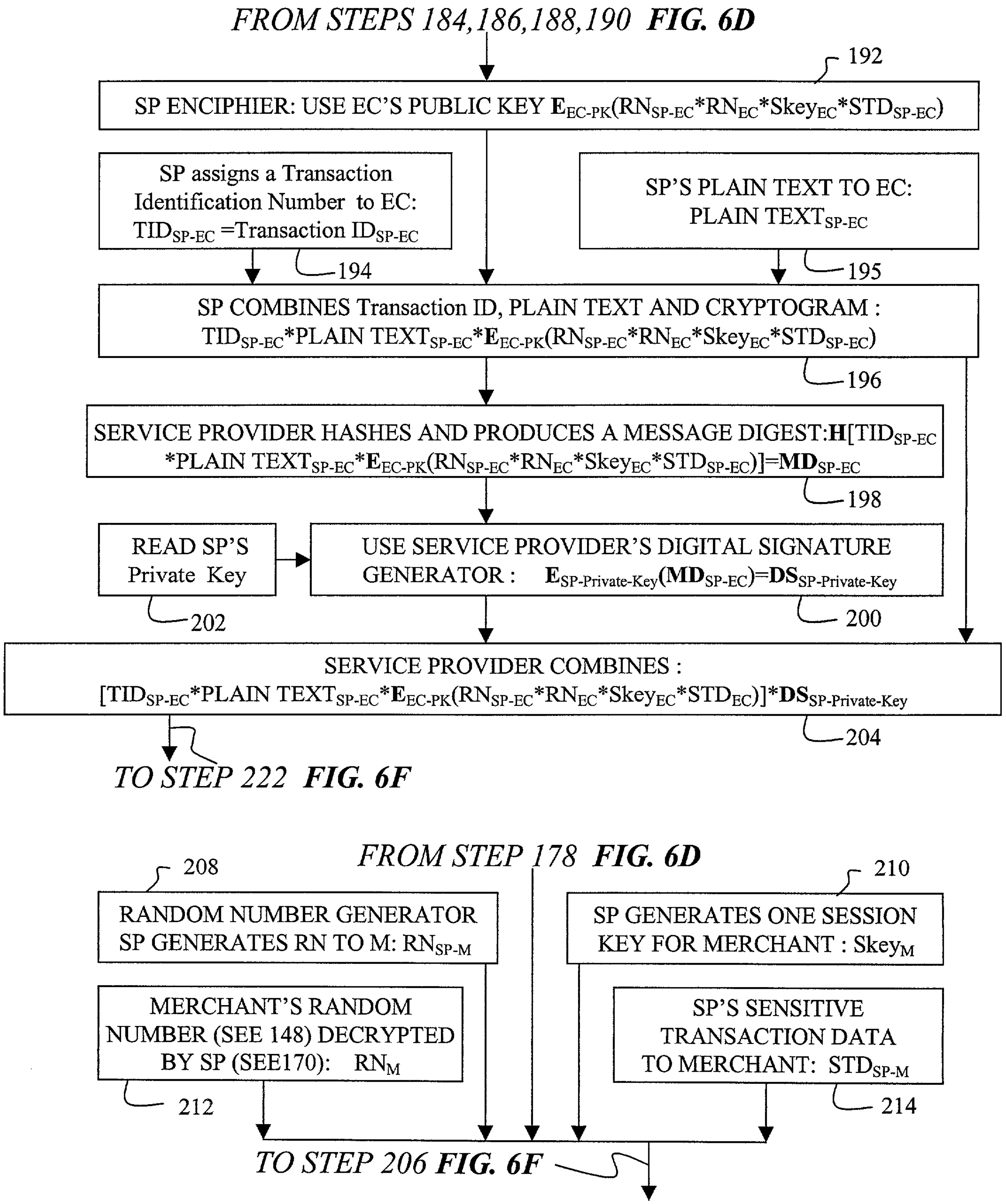

FROM STEPS 184,186,188,190 FIG. 6D
192
SP ENCIPHIER: USE EC'S PUBLIC KEY $\mathbf{E}_{EC\text{-}PK}(RN_{SP\text{-}EC}*RN_{EC}*Skey_{EC}*STD_{SP\text{-}EC})$
SP assigns a Transaction Identification Number to EC: $TID_{SP\text{-}EC}$ =Transaction $ID_{SP\text{-}EC}$
194
SP'S PLAIN TEXT TO EC: PLAIN $TEXT_{SP\text{-}EC}$
195
SP COMBINES Transaction ID, PLAIN TEXT AND CRYPTOGRAM : $TID_{SP\text{-}EC}$*PLAIN $TEXT_{SP\text{-}EC}*\mathbf{E}_{EC\text{-}PK}(RN_{SP\text{-}EC}*RN_{EC}*Skey_{EC}*STD_{SP\text{-}EC})$
196
SERVICE PROVIDER HASHES AND PRODUCES A MESSAGE DIGEST:$\mathbf{H}[TID_{SP\text{-}EC}$ *PLAIN $TEXT_{SP\text{-}EC}*\mathbf{E}_{EC\text{-}PK}(RN_{SP\text{-}EC}*RN_{EC}*Skey_{EC}*STD_{SP\text{-}EC})]=\mathbf{MD}_{SP\text{-}EC}$
198
READ SP'S Private Key
202
USE SERVICE PROVIDER'S DIGITAL SIGNATURE GENERATOR : $\mathbf{E}_{SP\text{-}Private\text{-}Key}(\mathbf{MD}_{SP\text{-}EC})=\mathbf{DS}_{SP\text{-}Private\text{-}Key}$
200
SERVICE PROVIDER COMBINES : $[TID_{SP\text{-}EC}$*PLAIN $TEXT_{SP\text{-}EC}*\mathbf{E}_{EC\text{-}PK}(RN_{SP\text{-}EC}*RN_{EC}*Skey_{EC}*STD_{EC})]*\mathbf{DS}_{SP\text{-}Private\text{-}Key}$
204
TO STEP 222 FIG. 6F
FROM STEP 178 FIG. 6D
208
RANDOM NUMBER GENERATOR SP GENERATES RN TO M: $RN_{SP\text{-}M}$
210
SP GENERATES ONE SESSION KEY FOR MERCHANT : $Skey_{M}$
MERCHANT'S RANDOM NUMBER (SEE 148) DECRYPTED BY SP (SEE170): RN_{M}
212
SP'S SENSITIVE TRANSACTION DATA TO MERCHANT: $STD_{SP\text{-}M}$
214
TO STEP 206 FIG. 6F

FIG. 6F

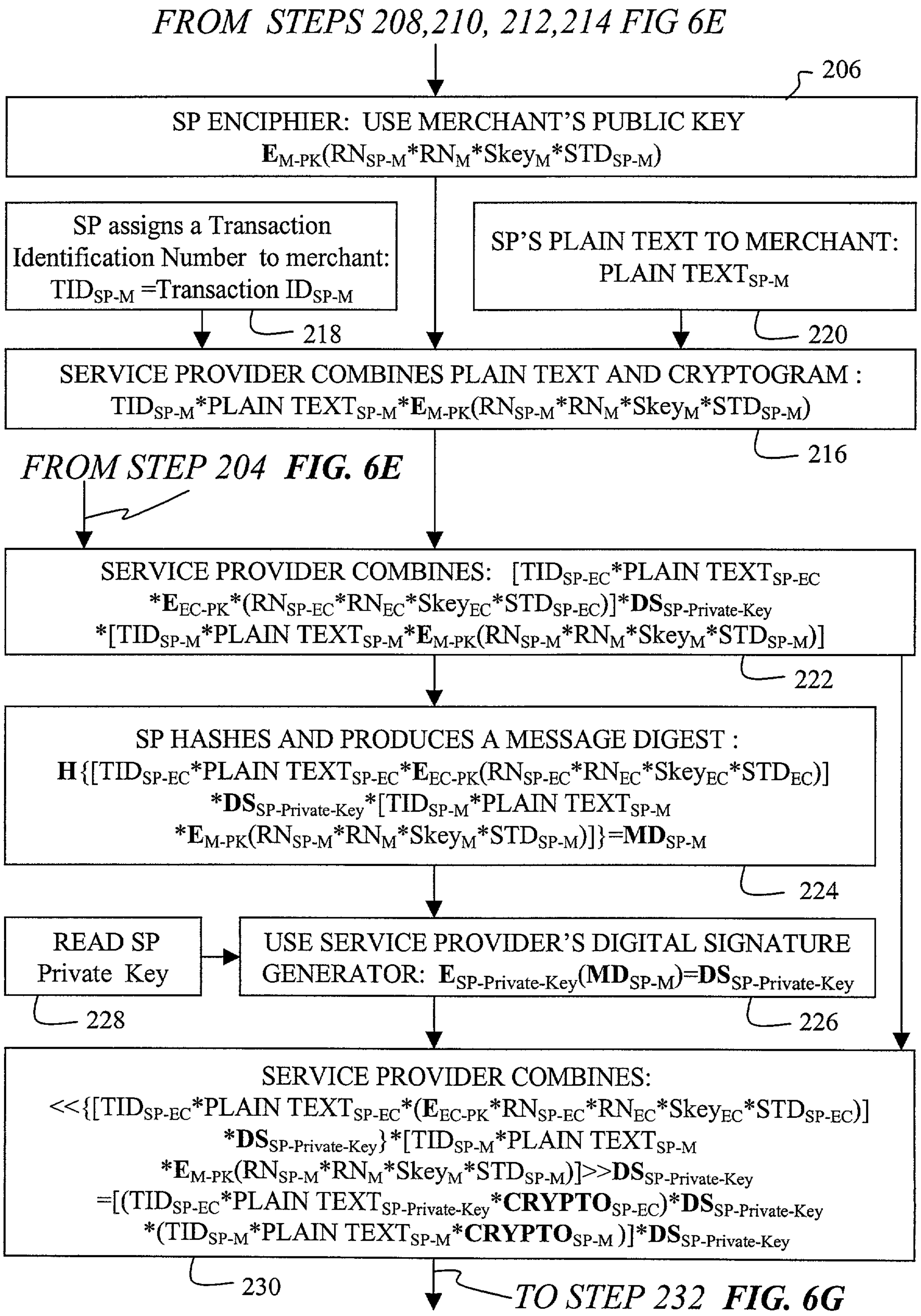

FROM STEPS 208,210, 212,214 FIG 6E
206
SP ENCIPHIER: USE MERCHANT'S PUBLIC KEY
$E_{M\text{-}PK}(RN_{SP\text{-}M}*RN_M*Skey_M*STD_{SP\text{-}M})$
SP assigns a Transaction Identification Number to merchant: $TID_{SP\text{-}M}$ =Transaction $ID_{SP\text{-}M}$
218
SP'S PLAIN TEXT TO MERCHANT: PLAIN $TEXT_{SP\text{-}M}$
220
SERVICE PROVIDER COMBINES PLAIN TEXT AND CRYPTOGRAM :
$TID_{SP\text{-}M}$*PLAIN $TEXT_{SP\text{-}M}*E_{M\text{-}PK}(RN_{SP\text{-}M}*RN_M*Skey_M*STD_{SP\text{-}M})$
216
FROM STEP 204 FIG. 6E
SERVICE PROVIDER COMBINES: $[TID_{SP\text{-}EC}$*PLAIN $TEXT_{SP\text{-}EC}$
$*E_{EC\text{-}PK}*(RN_{SP\text{-}EC}*RN_{EC}*Skey_{EC}*STD_{SP\text{-}EC})]*DS_{SP\text{-}Private\text{-}Key}$
$*[TID_{SP\text{-}M}$*PLAIN $TEXT_{SP\text{-}M}*E_{M\text{-}PK}(RN_{SP\text{-}M}*RN_M*Skey_M*STD_{SP\text{-}M})]$
222
SP HASHES AND PRODUCES A MESSAGE DIGEST :
$H\{[TID_{SP\text{-}EC}$*PLAIN $TEXT_{SP\text{-}EC}*E_{EC\text{-}PK}(RN_{SP\text{-}EC}*RN_{EC}*Skey_{EC}*STD_{EC})]$
$*DS_{SP\text{-}Private\text{-}Key}*[TID_{SP\text{-}M}$*PLAIN $TEXT_{SP\text{-}M}$
$*E_{M\text{-}PK}(RN_{SP\text{-}M}*RN_M*Skey_M*STD_{SP\text{-}M})]\}=MD_{SP\text{-}M}$
224
READ SP Private Key
228
USE SERVICE PROVIDER'S DIGITAL SIGNATURE GENERATOR: $E_{SP\text{-}Private\text{-}Key}(MD_{SP\text{-}M})=DS_{SP\text{-}Private\text{-}Key}$
226
SERVICE PROVIDER COMBINES:
$<<\{[TID_{SP\text{-}EC}$*PLAIN $TEXT_{SP\text{-}EC}*(E_{EC\text{-}PK}*RN_{SP\text{-}EC}*RN_{EC}*Skey_{EC}*STD_{SP\text{-}EC})]$
$*DS_{SP\text{-}Private\text{-}Key}\}*[TID_{SP\text{-}M}$*PLAIN $TEXT_{SP\text{-}M}$
$*E_{M\text{-}PK}(RN_{SP\text{-}M}*RN_M*Skey_M*STD_{SP\text{-}M})]>>DS_{SP\text{-}Private\text{-}Key}$
$=[(TID_{SP\text{-}EC}$*PLAIN $TEXT_{SP\text{-}Private\text{-}Key}*CRYPTO_{SP\text{-}EC})*DS_{SP\text{-}Private\text{-}Key}$
$*(TID_{SP\text{-}M}$*PLAIN $TEXT_{SP\text{-}M}*CRYPTO_{SP\text{-}M})]*DS_{SP\text{-}Private\text{-}Key}$
230
TO STEP 232 FIG. 6G

FIG. 6G

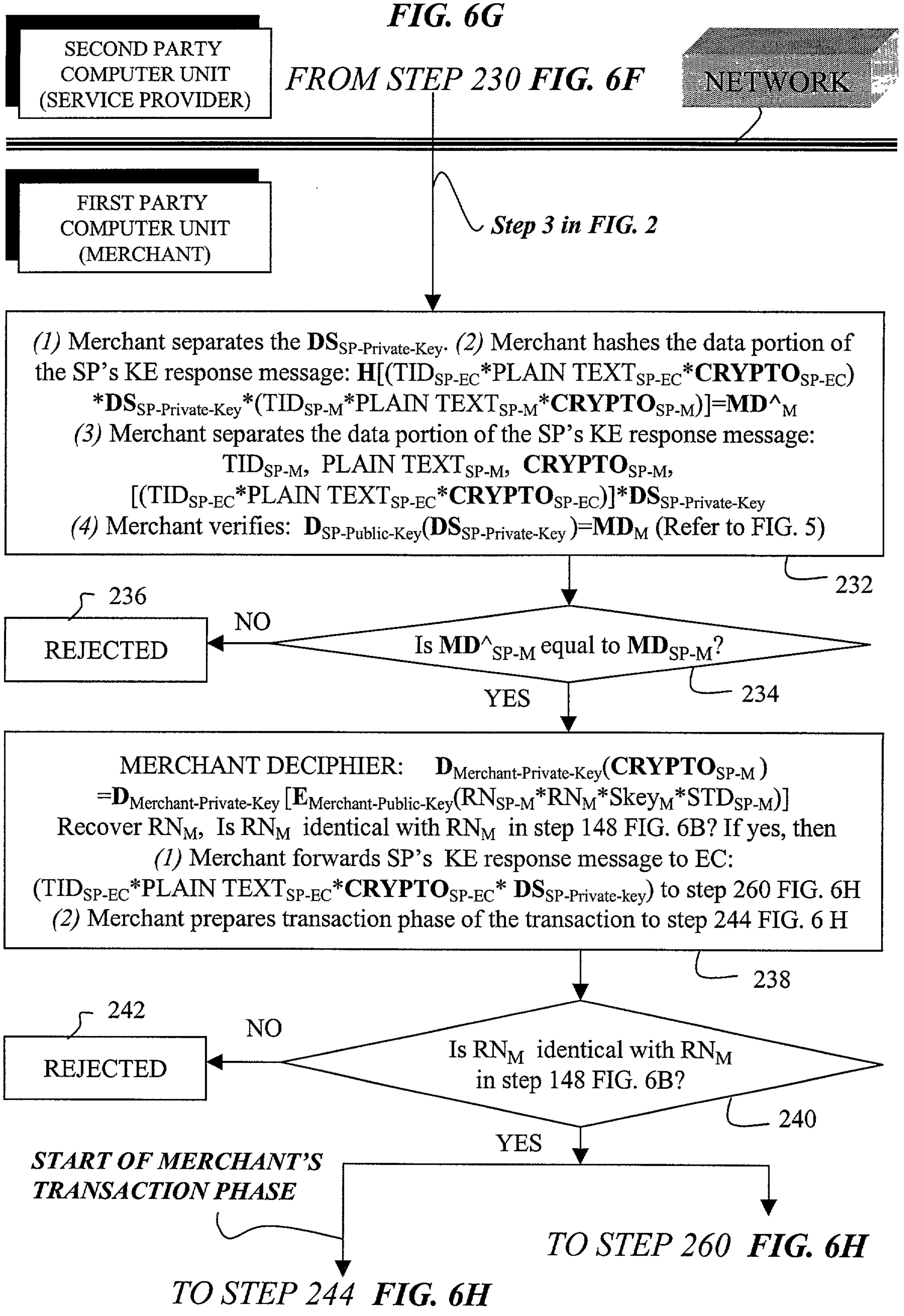

SECOND PARTY COMPUTER UNIT (SERVICE PROVIDER)
FROM STEP 230 FIG. 6F
NETWORK
FIRST PARTY COMPUTER UNIT (MERCHANT)
Step 3 in FIG. 2
(1) Merchant separates the $\mathbf{DS}_{SP\text{-}Private\text{-}Key}$. (2) Merchant hashes the data portion of the SP's KE response message: $\mathbf{H}[(TID_{SP\text{-}EC}*PLAIN\ TEXT_{SP\text{-}EC}*\mathbf{CRYPTO}_{SP\text{-}EC})*\mathbf{DS}_{SP\text{-}Private\text{-}Key}*(TID_{SP\text{-}M}*PLAIN\ TEXT_{SP\text{-}M}*\mathbf{CRYPTO}_{SP\text{-}M})]=\mathbf{MD}\text{^}_{M}$
(3) Merchant separates the data portion of the SP's KE response message: $TID_{SP\text{-}M}$, $PLAIN\ TEXT_{SP\text{-}M}$, $\mathbf{CRYPTO}_{SP\text{-}M}$, $[(TID_{SP\text{-}EC}*PLAIN\ TEXT_{SP\text{-}EC}*\mathbf{CRYPTO}_{SP\text{-}EC})]*\mathbf{DS}_{SP\text{-}Private\text{-}Key}$
(4) Merchant verifies: $\mathbf{D}_{SP\text{-}Public\text{-}Key}(\mathbf{DS}_{SP\text{-}Private\text{-}Key})=\mathbf{MD}_{M}$ (Refer to FIG. 5)
232
236
REJECTED
NO
Is $\mathbf{MD}\text{^}_{SP\text{-}M}$ equal to $\mathbf{MD}_{SP\text{-}M}$?
234
YES
MERCHANT DECIPHIER: $\mathbf{D}_{Merchant\text{-}Private\text{-}Key}(\mathbf{CRYPTO}_{SP\text{-}M})=\mathbf{D}_{Merchant\text{-}Private\text{-}Key}[\mathbf{E}_{Merchant\text{-}Public\text{-}Key}(RN_{SP\text{-}M}*RN_{M}*Skey_{M}*STD_{SP\text{-}M})]$
Recover RN_{M}, Is RN_{M} identical with RN_{M} in step 148 FIG. 6B? If yes, then
(1) Merchant forwards SP's KE response message to EC: $(TID_{SP\text{-}EC}*PLAIN\ TEXT_{SP\text{-}EC}*\mathbf{CRYPTO}_{SP\text{-}EC}*\ \mathbf{DS}_{SP\text{-}Private\text{-}key})$ to step 260 FIG. 6H
(2) Merchant prepares transaction phase of the transaction to step 244 FIG. 6 H
238
242
REJECTED
NO
Is RN_{M} identical with RN_{M} in step 148 FIG. 6B?
240
YES
START OF MERCHANT'S TRANSACTION PHASE
TO STEP 260 FIG. 6H
TO STEP 244 FIG. 6H

FIG. 6H

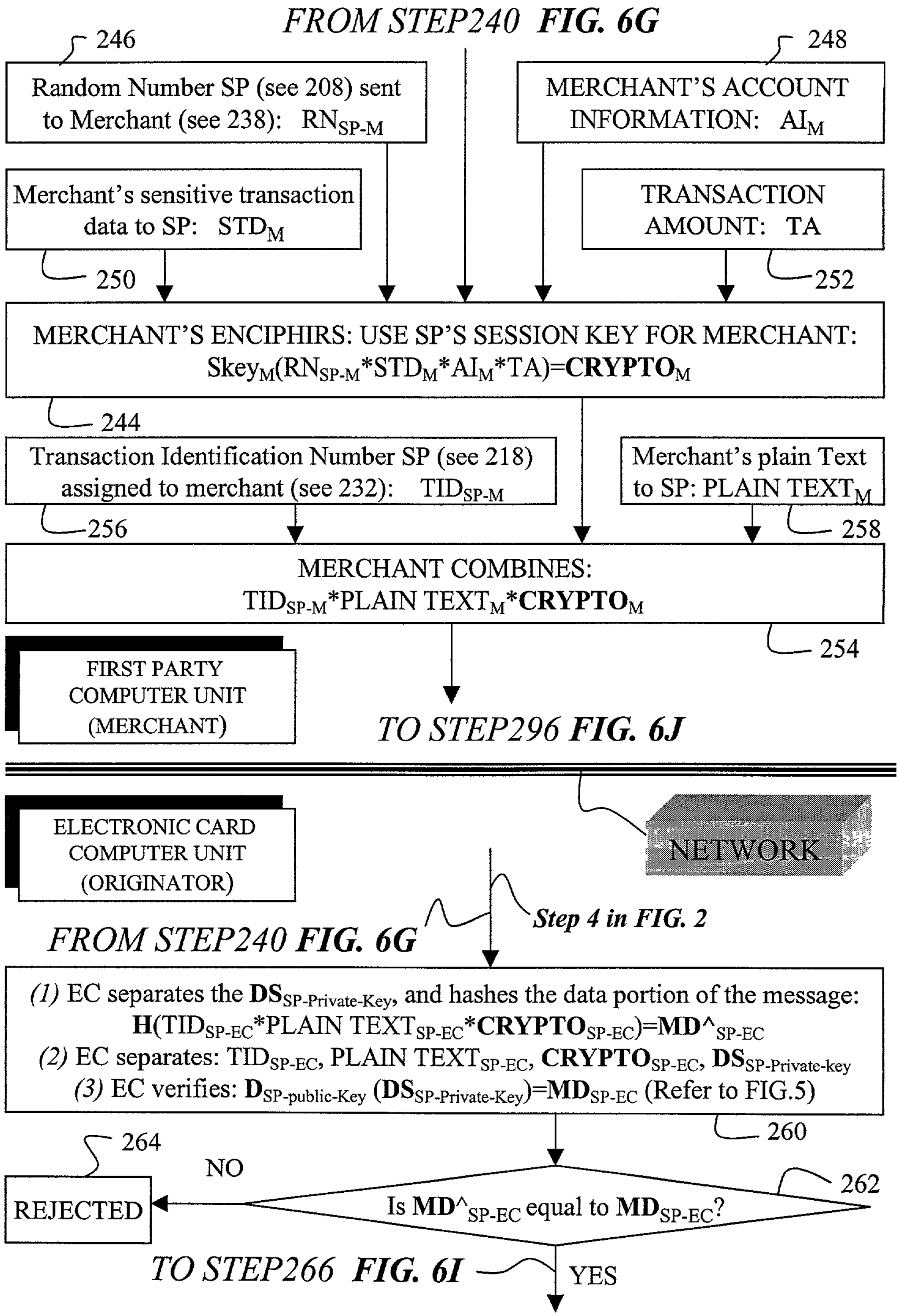
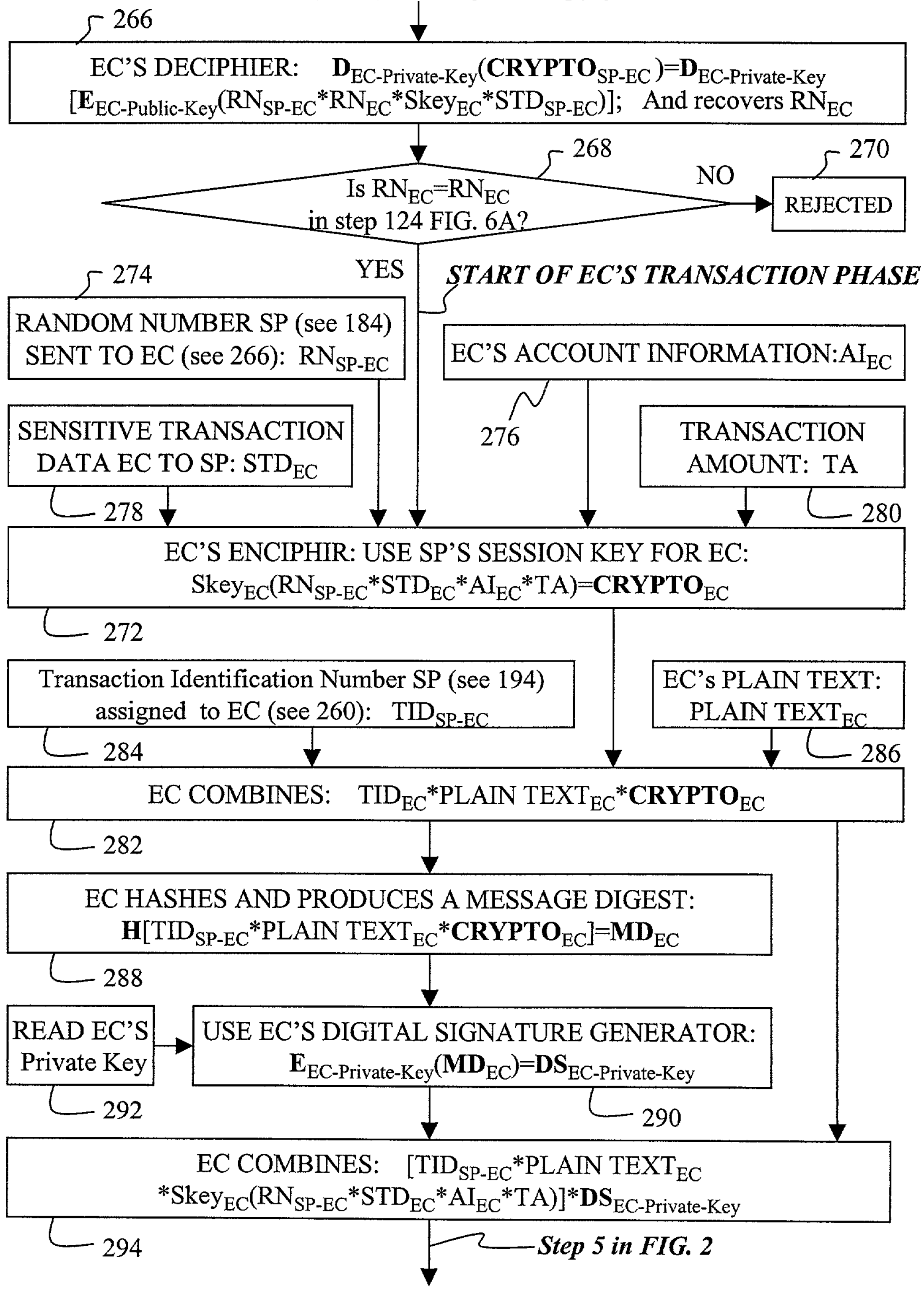

FROM STEP240 FIG. 6G
246
Random Number SP (see 208) sent to Merchant (see 238): RN_{SP-M}
248
MERCHANT'S ACCOUNT INFORMATION: AI_M
Merchant's sensitive transaction data to SP: STD_M
TRANSACTION AMOUNT: TA
250
252
MERCHANT'S ENCIPHIRS: USE SP'S SESSION KEY FOR MERCHANT: $Skey_M(RN_{SP-M}*STD_M*AI_M*TA)=\mathbf{CRYPTO}_M$
244
Transaction Identification Number SP (see 218) assigned to merchant (see 232): TID_{SP-M}
Merchant's plain Text to SP: PLAIN $TEXT_M$
256
258
MERCHANT COMBINES: $TID_{SP-M}*PLAIN\ TEXT_M*\mathbf{CRYPTO}_M$
254
FIRST PARTY COMPUTER UNIT (MERCHANT)
TO STEP296 FIG. 6J
NETWORK
ELECTRONIC CARD COMPUTER UNIT (ORIGINATOR)
Step 4 in FIG. 2
FROM STEP240 FIG. 6G
(1) EC separates the $\mathbf{DS}_{SP-Private-Key}$, and hashes the data portion of the message: $\mathbf{H}(TID_{SP-EC}*PLAIN\ TEXT_{SP-EC}*\mathbf{CRYPTO}_{SP-EC})=\mathbf{MD}\hat{}_{SP-EC}$
(2) EC separates: TID_{SP-EC}, PLAIN $TEXT_{SP-EC}$, $\mathbf{CRYPTO}_{SP-EC}$, $\mathbf{DS}_{SP-Private-key}$
(3) EC verifies: $\mathbf{D}_{SP-public-Key}(\mathbf{DS}_{SP-Private-Key})=\mathbf{MD}_{SP-EC}$ (Refer to FIG.5)
260
264
NO
262
REJECTED
Is $\mathbf{MD}\hat{}_{SP-EC}$ equal to $\mathbf{MD}_{SP-EC}$?
TO STEP266 FIG. 6I
YES

FIG. 6I

FROM STEP262 ***FIG. 6H***


266
EC'S DECIPHIER: $\mathbf{D}_{EC\text{-}Private\text{-}Key}(\mathbf{CRYPTO}_{SP\text{-}EC})=\mathbf{D}_{EC\text{-}Private\text{-}Key}$
$[\mathbf{E}_{EC\text{-}Public\text{-}Key}(RN_{SP\text{-}EC}*RN_{EC}*Skey_{EC}*STD_{SP\text{-}EC})]$; And recovers RN_{EC}
268
Is $RN_{EC}=RN_{EC}$ in step 124 FIG. 6A?
NO
270
REJECTED
YES
START OF EC'S TRANSACTION PHASE
274
RANDOM NUMBER SP (see 184) SENT TO EC (see 266): $RN_{SP\text{-}EC}$
EC'S ACCOUNT INFORMATION:AI_{EC}
276
SENSITIVE TRANSACTION DATA EC TO SP: STD_{EC}
TRANSACTION AMOUNT: TA
278
280
EC'S ENCIPHIR: USE SP'S SESSION KEY FOR EC:
$Skey_{EC}(RN_{SP\text{-}EC}*STD_{EC}*AI_{EC}*TA)=\mathbf{CRYPTO}_{EC}$
272
Transaction Identification Number SP (see 194) assigned to EC (see 260): $TID_{SP\text{-}EC}$
EC's PLAIN TEXT: PLAIN $TEXT_{EC}$
284
286
EC COMBINES: TID_{EC}*PLAIN $TEXT_{EC}*\mathbf{CRYPTO}_{EC}$
282
EC HASHES AND PRODUCES A MESSAGE DIGEST:
$\mathbf{H}[TID_{SP\text{-}EC}$*PLAIN $TEXT_{EC}*\mathbf{CRYPTO}_{EC}]=\mathbf{MD}_{EC}$
288
READ EC'S Private Key
USE EC'S DIGITAL SIGNATURE GENERATOR:
$\mathbf{E}_{EC\text{-}Private\text{-}Key}(\mathbf{MD}_{EC})=\mathbf{DS}_{EC\text{-}Private\text{-}Key}$
292
290
EC COMBINES: $[TID_{SP\text{-}EC}$*PLAIN $TEXT_{EC}$
$*Skey_{EC}(RN_{SP\text{-}EC}*STD_{EC}*AI_{EC}*TA)]*\mathbf{DS}_{EC\text{-}Private\text{-}Key}$
294
Step 5 in FIG. 2

TO STEP296 ***FIG. 6J***

FIG. 6J

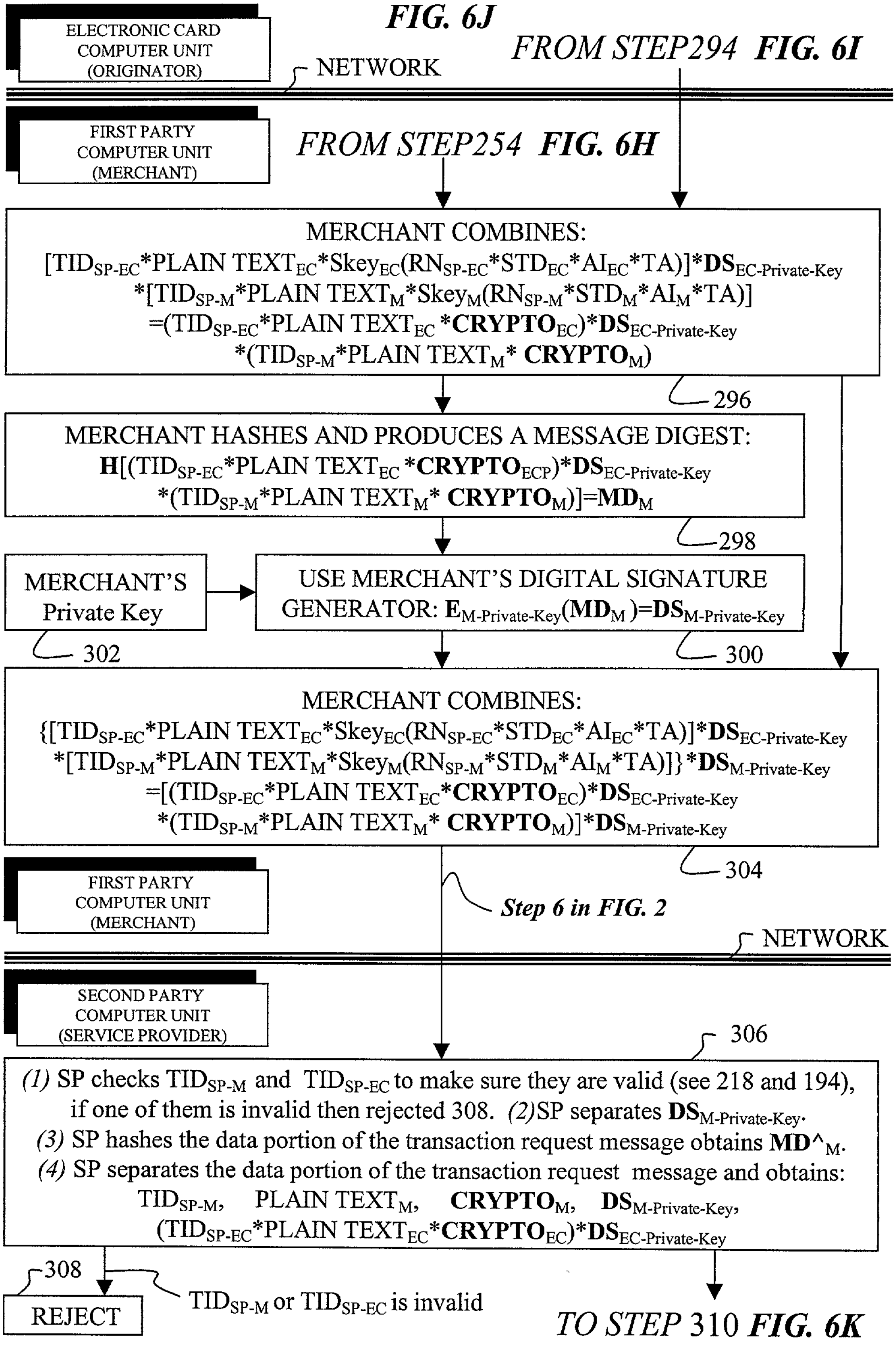

ELECTRONIC CARD COMPUTER UNIT (ORIGINATOR)
NETWORK
FROM STEP294 FIG. 6I
FIRST PARTY COMPUTER UNIT (MERCHANT)
FROM STEP254 FIG. 6H
MERCHANT COMBINES:
$[TID_{SP\text{-}EC}*PLAIN\ TEXT_{EC}*Skey_{EC}(RN_{SP\text{-}EC}*STD_{EC}*AI_{EC}*TA)]*\mathbf{DS}_{EC\text{-}Private\text{-}Key}$
$*[TID_{SP\text{-}M}*PLAIN\ TEXT_{M}*Skey_{M}(RN_{SP\text{-}M}*STD_{M}*AI_{M}*TA)]$
$=(TID_{SP\text{-}EC}*PLAIN\ TEXT_{EC}*\mathbf{CRYPTO}_{EC})*\mathbf{DS}_{EC\text{-}Private\text{-}Key}$
$*(TID_{SP\text{-}M}*PLAIN\ TEXT_{M}*\mathbf{CRYPTO}_{M})$
296
MERCHANT HASHES AND PRODUCES A MESSAGE DIGEST:
$\mathbf{H}[(TID_{SP\text{-}EC}*PLAIN\ TEXT_{EC}*\mathbf{CRYPTO}_{ECP})*\mathbf{DS}_{EC\text{-}Private\text{-}Key}$
$*(TID_{SP\text{-}M}*PLAIN\ TEXT_{M}*\mathbf{CRYPTO}_{M})]=\mathbf{MD}_{M}$
298
MERCHANT'S Private Key
USE MERCHANT'S DIGITAL SIGNATURE GENERATOR: $\mathbf{E}_{M\text{-}Private\text{-}Key}(\mathbf{MD}_{M})=\mathbf{DS}_{M\text{-}Private\text{-}Key}$
302
300
MERCHANT COMBINES:
$\{[TID_{SP\text{-}EC}*PLAIN\ TEXT_{EC}*Skey_{EC}(RN_{SP\text{-}EC}*STD_{EC}*AI_{EC}*TA)]*\mathbf{DS}_{EC\text{-}Private\text{-}Key}$
$*[TID_{SP\text{-}M}*PLAIN\ TEXT_{M}*Skey_{M}(RN_{SP\text{-}M}*STD_{M}*AI_{M}*TA)]\}*\mathbf{DS}_{M\text{-}Private\text{-}Key}$
$=[(TID_{SP\text{-}EC}*PLAIN\ TEXT_{EC}*\mathbf{CRYPTO}_{EC})*\mathbf{DS}_{EC\text{-}Private\text{-}Key}$
$*(TID_{SP\text{-}M}*PLAIN\ TEXT_{M}*\mathbf{CRYPTO}_{M})]*\mathbf{DS}_{M\text{-}Private\text{-}Key}$
304
FIRST PARTY COMPUTER UNIT (MERCHANT)
Step 6 in FIG. 2
NETWORK
SECOND PARTY COMPUTER UNIT (SERVICE PROVIDER)
306
(1) SP checks $TID_{SP\text{-}M}$ and $TID_{SP\text{-}EC}$ to make sure they are valid (see 218 and 194),
if one of them is invalid then rejected 308. (2)SP separates $\mathbf{DS}_{M\text{-}Private\text{-}Key}$.
(3) SP hashes the data portion of the transaction request message obtains $\mathbf{MD}^{\wedge}_{M}$.
(4) SP separates the data portion of the transaction request message and obtains:
$TID_{SP\text{-}M}$, $PLAIN\ TEXT_{M}$, $\mathbf{CRYPTO}_{M}$, $\mathbf{DS}_{M\text{-}Private\text{-}Key}$,
$(TID_{SP\text{-}EC}*PLAIN\ TEXT_{EC}*\mathbf{CRYPTO}_{EC})*\mathbf{DS}_{EC\text{-}Private\text{-}Key}$
308
REJECT
$TID_{SP\text{-}M}$ or $TID_{SP\text{-}EC}$ is invalid
TO STEP 310 FIG. 6K

FIG. 6K

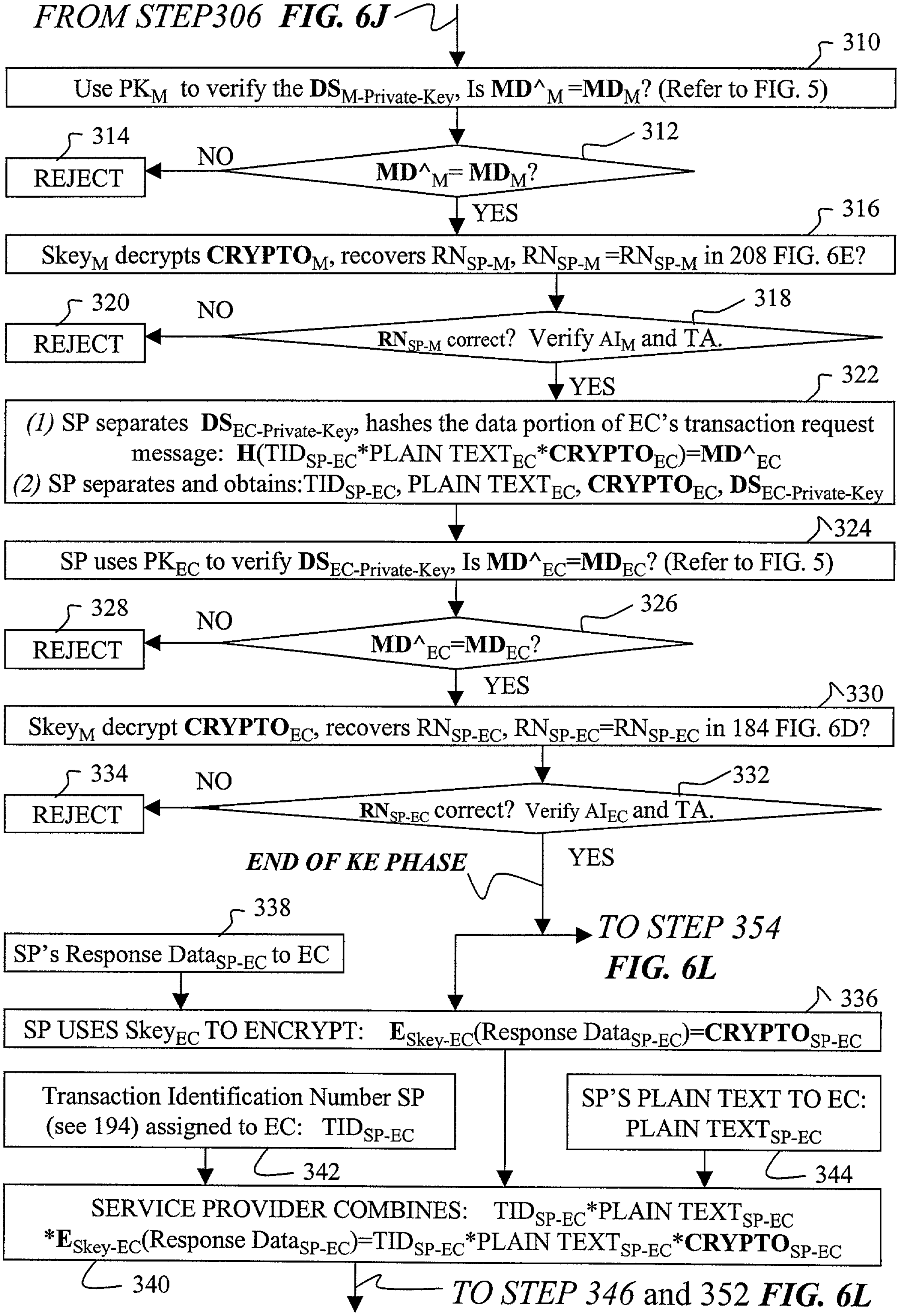

FROM STEP306 FIG. 6J
310
Use PK$_M$ to verify the **DS**$_{M\text{-Private-Key}}$, Is **MD^**$_M$=**MD**$_M$? (Refer to FIG. 5)
312
314
REJECT
NO
MD^$_M$= **MD**$_M$?
YES
316
Skey$_M$ decrypts **CRYPTO**$_M$, recovers RN$_{SP\text{-}M}$, RN$_{SP\text{-}M}$=RN$_{SP\text{-}M}$ in 208 FIG. 6E?
318
320
REJECT
NO
RN$_{SP\text{-}M}$ correct? Verify AI$_M$ and TA.
YES
322
(1) SP separates **DS**$_{EC\text{-Private-Key}}$, hashes the data portion of EC's transaction request message: **H**(TID$_{SP\text{-}EC}$*PLAIN TEXT$_{EC}$***CRYPTO**$_{EC}$)=**MD^**$_{EC}$
(2) SP separates and obtains:TID$_{SP\text{-}EC}$, PLAIN TEXT$_{EC}$, **CRYPTO**$_{EC}$, **DS**$_{EC\text{-Private-Key}}$
324
SP uses PK$_{EC}$ to verify **DS**$_{EC\text{-Private-Key}}$, Is **MD^**$_{EC}$=**MD**$_{EC}$? (Refer to FIG. 5)
326
328
REJECT
NO
MD^$_{EC}$=**MD**$_{EC}$?
YES
330
Skey$_M$ decrypt **CRYPTO**$_{EC}$, recovers RN$_{SP\text{-}EC}$, RN$_{SP\text{-}EC}$=RN$_{SP\text{-}EC}$ in 184 FIG. 6D?
332
334
REJECT
NO
RN$_{SP\text{-}EC}$ correct? Verify AI$_{EC}$ and TA.
YES
END OF KE PHASE
TO STEP 354 FIG. 6L
338
SP's Response Data$_{SP\text{-}EC}$ to EC
336
SP USES Skey$_{EC}$ TO ENCRYPT: E$_{Skey\text{-}EC}$(Response Data$_{SP\text{-}EC}$)=**CRYPTO**$_{SP\text{-}EC}$
Transaction Identification Number SP (see 194) assigned to EC: TID$_{SP\text{-}EC}$
342
SP'S PLAIN TEXT TO EC: PLAIN TEXT$_{SP\text{-}EC}$
344
SERVICE PROVIDER COMBINES: TID$_{SP\text{-}EC}$*PLAIN TEXT$_{SP\text{-}EC}$ ***E**$_{Skey\text{-}EC}$(Response Data$_{SP\text{-}EC}$)=TID$_{SP\text{-}EC}$*PLAIN TEXT$_{SP\text{-}EC}$***CRYPTO**$_{SP\text{-}EC}$
340
TO STEP 346 and 352 FIG. 6L

FIG. 6L

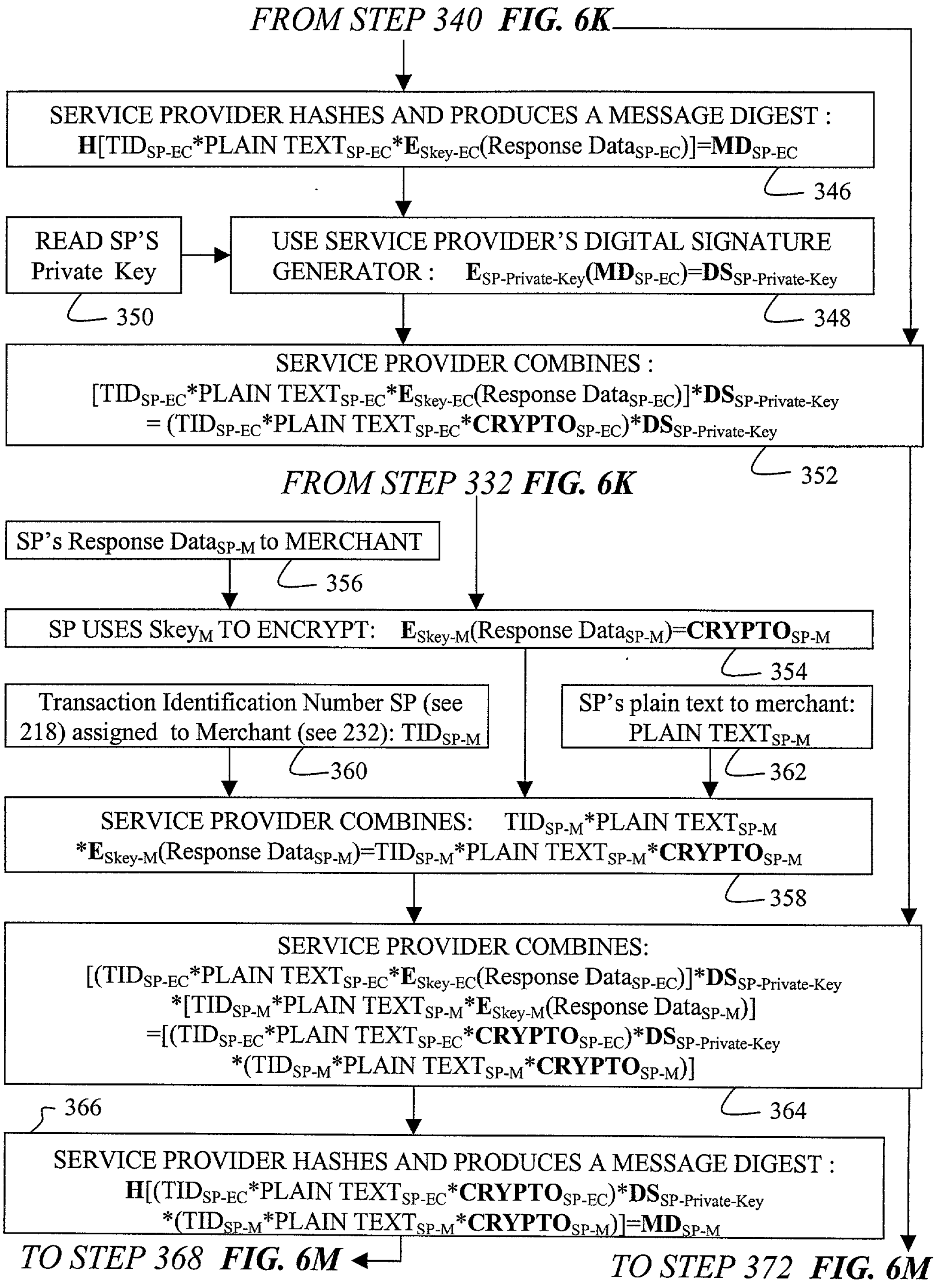

FROM STEP 340 FIG. 6K
SERVICE PROVIDER HASHES AND PRODUCES A MESSAGE DIGEST : H[TID_SP-EC*PLAIN TEXT_SP-EC*E_Skey-EC(Response Data_SP-EC)]=MD_SP-EC
346
READ SP'S Private Key
350
USE SERVICE PROVIDER'S DIGITAL SIGNATURE GENERATOR : E_SP-Private-Key(MD_SP-EC)=DS_SP-Private-Key
348
SERVICE PROVIDER COMBINES : [TID_SP-EC*PLAIN TEXT_SP-EC*E_Skey-EC(Response Data_SP-EC)]*DS_SP-Private-Key = (TID_SP-EC*PLAIN TEXT_SP-EC*CRYPTO_SP-EC)*DS_SP-Private-Key
352
FROM STEP 332 FIG. 6K
SP's Response Data_SP-M to MERCHANT
356
SP USES Skey_M TO ENCRYPT: E_Skey-M(Response Data_SP-M)=CRYPTO_SP-M
354
Transaction Identification Number SP (see 218) assigned to Merchant (see 232): TID_SP-M
360
SP's plain text to merchant: PLAIN TEXT_SP-M
362
SERVICE PROVIDER COMBINES: TID_SP-M*PLAIN TEXT_SP-M *E_Skey-M(Response Data_SP-M)=TID_SP-M*PLAIN TEXT_SP-M*CRYPTO_SP-M
358
SERVICE PROVIDER COMBINES: [(TID_SP-EC*PLAIN TEXT_SP-EC*E_Skey-EC(Response Data_SP-EC)]*DS_SP-Private-Key *[TID_SP-M*PLAIN TEXT_SP-M*E_Skey-M(Response Data_SP-M)] =[(TID_SP-EC*PLAIN TEXT_SP-EC*CRYPTO_SP-EC)*DS_SP-Private-Key *(TID_SP-M*PLAIN TEXT_SP-M*CRYPTO_SP-M)]
364
366
SERVICE PROVIDER HASHES AND PRODUCES A MESSAGE DIGEST : H[(TID_SP-EC*PLAIN TEXT_SP-EC*CRYPTO_SP-EC)*DS_SP-Private-Key *(TID_SP-M*PLAIN TEXT_SP-M*CRYPTO_SP-M)]=MD_SP-M
TO STEP 368 FIG. 6M
TO STEP 372 FIG. 6M

FIG. 6M

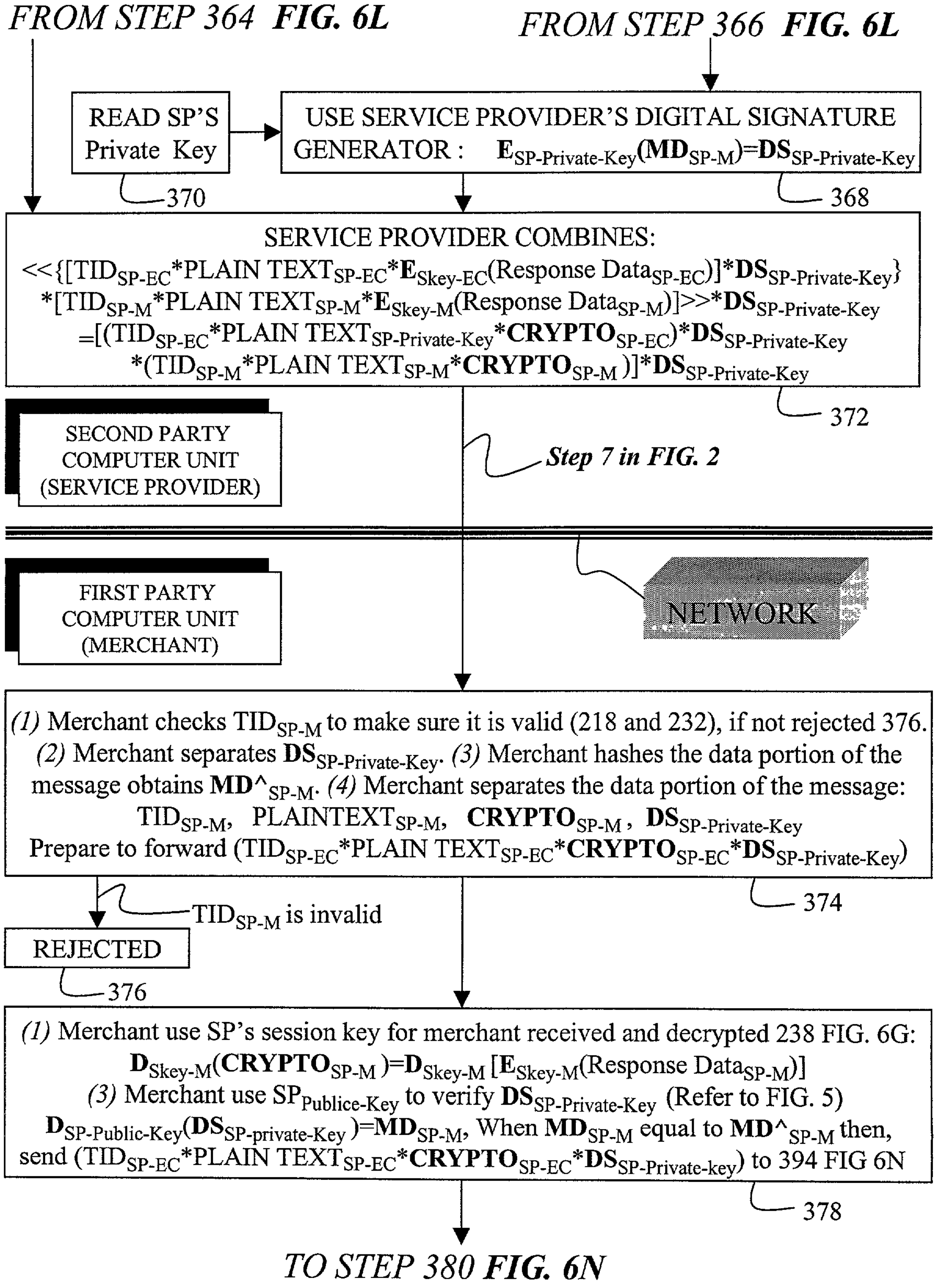

FROM STEP 364 FIG. 6L
FROM STEP 366 FIG. 6L
READ SP'S Private Key
370
USE SERVICE PROVIDER'S DIGITAL SIGNATURE GENERATOR : $\mathbf{E}_{\text{SP-Private-Key}}(\mathbf{MD}_{\text{SP-M}})=\mathbf{DS}_{\text{SP-Private-Key}}$
368
SERVICE PROVIDER COMBINES:
$<<\{[\text{TID}_{\text{SP-EC}}*\text{PLAIN TEXT}_{\text{SP-EC}}*\mathbf{E}_{\text{Skey-EC}}(\text{Response Data}_{\text{SP-EC}})]*\mathbf{DS}_{\text{SP-Private-Key}}\}$
$*[\text{TID}_{\text{SP-M}}*\text{PLAIN TEXT}_{\text{SP-M}}*\mathbf{E}_{\text{Skey-M}}(\text{Response Data}_{\text{SP-M}})]>>*\mathbf{DS}_{\text{SP-Private-Key}}$
$=[(\text{TID}_{\text{SP-EC}}*\text{PLAIN TEXT}_{\text{SP-Private-Key}}*\mathbf{CRYPTO}_{\text{SP-EC}})*\mathbf{DS}_{\text{SP-Private-Key}}$
$*(\text{TID}_{\text{SP-M}}*\text{PLAIN TEXT}_{\text{SP-M}}*\mathbf{CRYPTO}_{\text{SP-M}})]*\mathbf{DS}_{\text{SP-Private-Key}}$
372
SECOND PARTY COMPUTER UNIT (SERVICE PROVIDER)
Step 7 in FIG. 2
FIRST PARTY COMPUTER UNIT (MERCHANT)
NETWORK
(1) Merchant checks $\text{TID}_{\text{SP-M}}$ to make sure it is valid (218 and 232), if not rejected 376. (2) Merchant separates $\mathbf{DS}_{\text{SP-Private-Key}}$. (3) Merchant hashes the data portion of the message obtains $\mathbf{MD}\hat{}_{\text{SP-M}}$. (4) Merchant separates the data portion of the message:
$\text{TID}_{\text{SP-M}}$, $\text{PLAINTEXT}_{\text{SP-M}}$, $\mathbf{CRYPTO}_{\text{SP-M}}$, $\mathbf{DS}_{\text{SP-Private-Key}}$
Prepare to forward $(\text{TID}_{\text{SP-EC}}*\text{PLAIN TEXT}_{\text{SP-EC}}*\mathbf{CRYPTO}_{\text{SP-EC}}*\mathbf{DS}_{\text{SP-Private-Key}})$
374
$\text{TID}_{\text{SP-M}}$ is invalid
REJECTED
376
(1) Merchant use SP's session key for merchant received and decrypted 238 FIG. 6G:
$\mathbf{D}_{\text{Skey-M}}(\mathbf{CRYPTO}_{\text{SP-M}})=\mathbf{D}_{\text{Skey-M}}[\mathbf{E}_{\text{Skey-M}}(\text{Response Data}_{\text{SP-M}})]$
(3) Merchant use $\text{SP}_{\text{Publice-Key}}$ to verify $\mathbf{DS}_{\text{SP-Private-Key}}$ (Refer to FIG. 5)
$\mathbf{D}_{\text{SP-Public-Key}}(\mathbf{DS}_{\text{SP-private-Key}})=\mathbf{MD}_{\text{SP-M}}$, When $\mathbf{MD}_{\text{SP-M}}$ equal to $\mathbf{MD}\hat{}_{\text{SP-M}}$ then, send $(\text{TID}_{\text{SP-EC}}*\text{PLAIN TEXT}_{\text{SP-EC}}*\mathbf{CRYPTO}_{\text{SP-EC}}*\mathbf{DS}_{\text{SP-Private-key}})$ to 394 FIG 6N
378
TO STEP 380 FIG. 6N

FIG. 6N

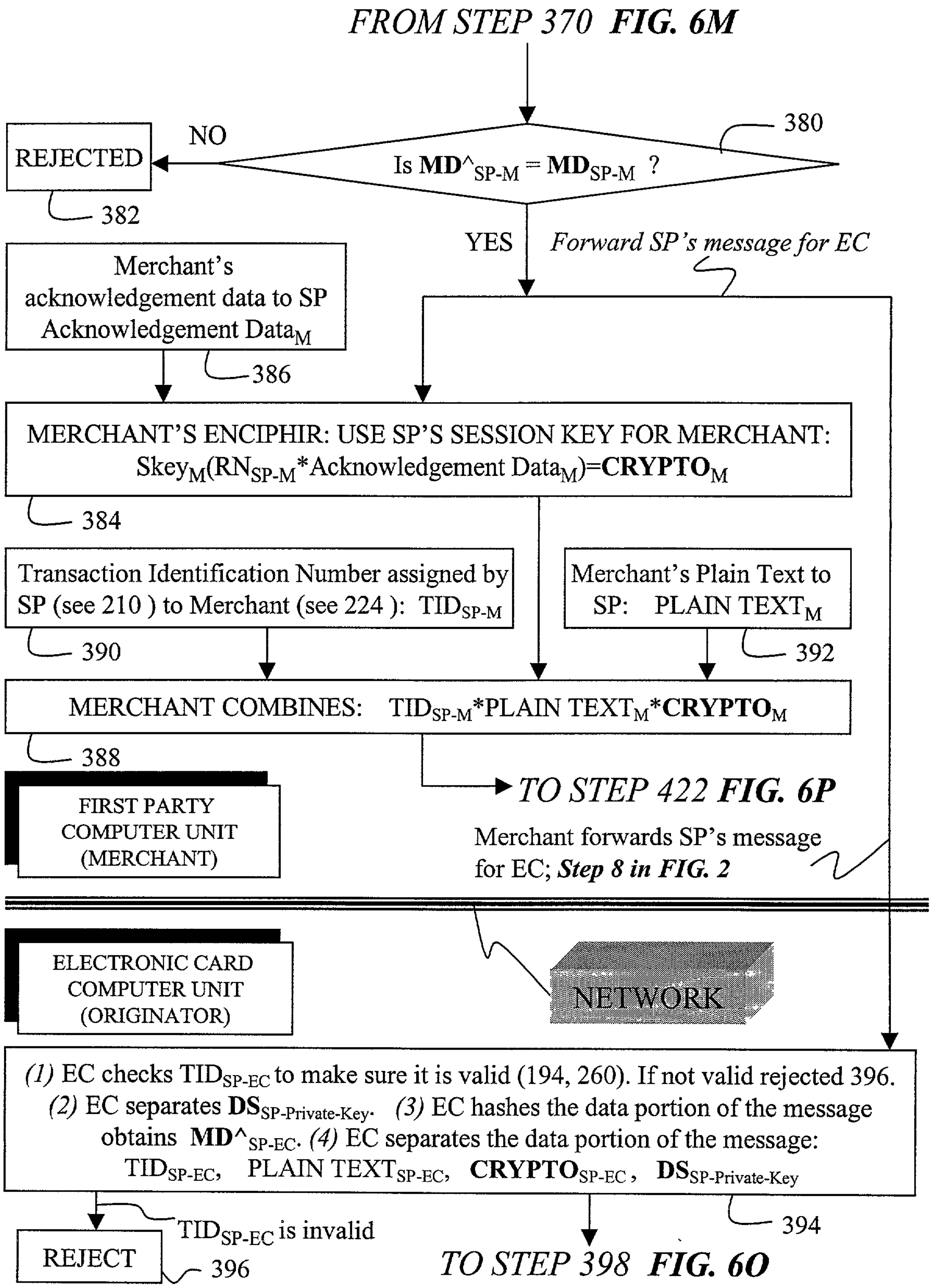

FROM STEP 370 FIG. 6M
Is $\mathbf{MD}^{\wedge}_{SP\text{-}M} = \mathbf{MD}_{SP\text{-}M}$?
380
NO
REJECTED
382
YES
Forward SP's message for EC
Merchant's acknowledgement data to SP Acknowledgement $Data_M$
386
MERCHANT'S ENCIPHIR: USE SP'S SESSION KEY FOR MERCHANT:
$Skey_M(RN_{SP\text{-}M}$*Acknowledgement $Data_M) = \mathbf{CRYPTO}_M$
384
Transaction Identification Number assigned by SP (see 210) to Merchant (see 224): $TID_{SP\text{-}M}$
390
Merchant's Plain Text to SP: PLAIN $TEXT_M$
392
MERCHANT COMBINES: $TID_{SP\text{-}M}$*PLAIN $TEXT_M$*$\mathbf{CRYPTO}_M$
388
FIRST PARTY COMPUTER UNIT (MERCHANT)
TO STEP 422 FIG. 6P
Merchant forwards SP's message for EC; Step 8 in FIG. 2
ELECTRONIC CARD COMPUTER UNIT (ORIGINATOR)
NETWORK
(1) EC checks $TID_{SP\text{-}EC}$ to make sure it is valid (194, 260). If not valid rejected 396.
(2) EC separates $\mathbf{DS}_{SP\text{-}Private\text{-}Key}$. (3) EC hashes the data portion of the message obtains $\mathbf{MD}^{\wedge}_{SP\text{-}EC}$. (4) EC separates the data portion of the message:
$TID_{SP\text{-}EC}$, PLAIN $TEXT_{SP\text{-}EC}$, $\mathbf{CRYPTO}_{SP\text{-}EC}$, $\mathbf{DS}_{SP\text{-}Private\text{-}Key}$
394
$TID_{SP\text{-}EC}$ is invalid
REJECT
396
TO STEP 398 FIG. 6O

FIG. 6O

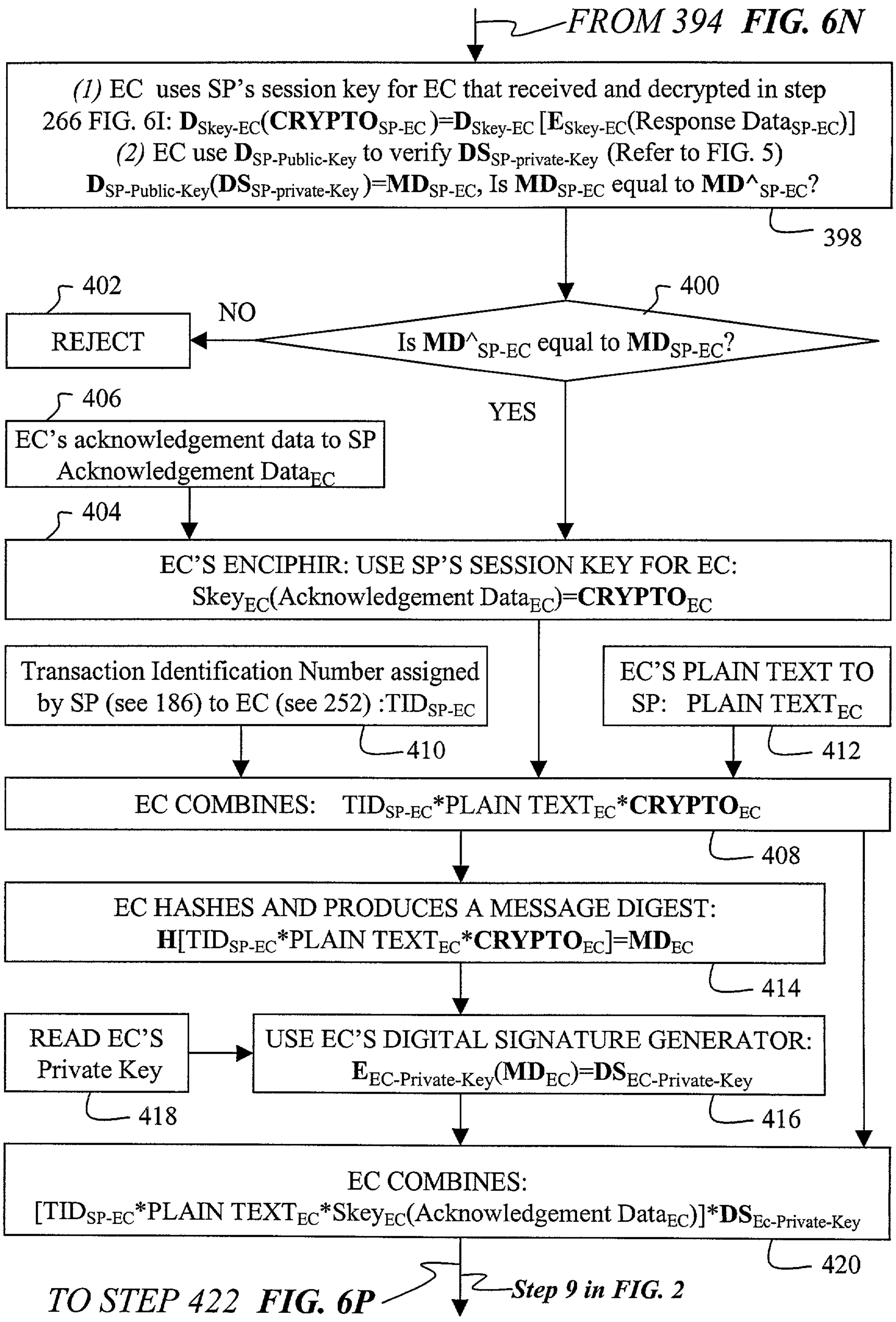

FROM 394 FIG. 6N
(1) EC uses SP's session key for EC that received and decrypted in step 266 FIG. 6I: $\mathbf{D}_{Skey\text{-}EC}(\mathbf{CRYPTO}_{SP\text{-}EC})=\mathbf{D}_{Skey\text{-}EC}[\mathbf{E}_{Skey\text{-}EC}(\text{Response Data}_{SP\text{-}EC})]$
(2) EC use $\mathbf{D}_{SP\text{-}Public\text{-}Key}$ to verify $\mathbf{DS}_{SP\text{-}private\text{-}Key}$ (Refer to FIG. 5)
$\mathbf{D}_{SP\text{-}Public\text{-}Key}(\mathbf{DS}_{SP\text{-}private\text{-}Key})=\mathbf{MD}_{SP\text{-}EC}$, Is $\mathbf{MD}_{SP\text{-}EC}$ equal to $\mathbf{MD}\hat{}_{SP\text{-}EC}$?
398
402
REJECT
NO
400
Is $\mathbf{MD}\hat{}_{SP\text{-}EC}$ equal to $\mathbf{MD}_{SP\text{-}EC}$?
406
EC's acknowledgement data to SP Acknowledgement Data_{EC}
YES
404
EC'S ENCIPHIR: USE SP'S SESSION KEY FOR EC:
$\text{Skey}_{EC}(\text{Acknowledgement Data}_{EC})=\mathbf{CRYPTO}_{EC}$
Transaction Identification Number assigned by SP (see 186) to EC (see 252) :$\text{TID}_{SP\text{-}EC}$
410
EC'S PLAIN TEXT TO SP: PLAIN TEXT_{EC}
412
EC COMBINES: $\text{TID}_{SP\text{-}EC}*\text{PLAIN TEXT}_{EC}*\mathbf{CRYPTO}_{EC}$
408
EC HASHES AND PRODUCES A MESSAGE DIGEST:
$\mathbf{H}[\text{TID}_{SP\text{-}EC}*\text{PLAIN TEXT}_{EC}*\mathbf{CRYPTO}_{EC}]=\mathbf{MD}_{EC}$
414
READ EC'S Private Key
418
USE EC'S DIGITAL SIGNATURE GENERATOR:
$\mathbf{E}_{EC\text{-}Private\text{-}Key}(\mathbf{MD}_{EC})=\mathbf{DS}_{EC\text{-}Private\text{-}Key}$
416
EC COMBINES:
$[\text{TID}_{SP\text{-}EC}*\text{PLAIN TEXT}_{EC}*\text{Skey}_{EC}(\text{Acknowledgement Data}_{EC})]*\mathbf{DS}_{Ec\text{-}Private\text{-}Key}$
420
TO STEP 422 FIG. 6P
Step 9 in FIG. 2

FIG. 6P

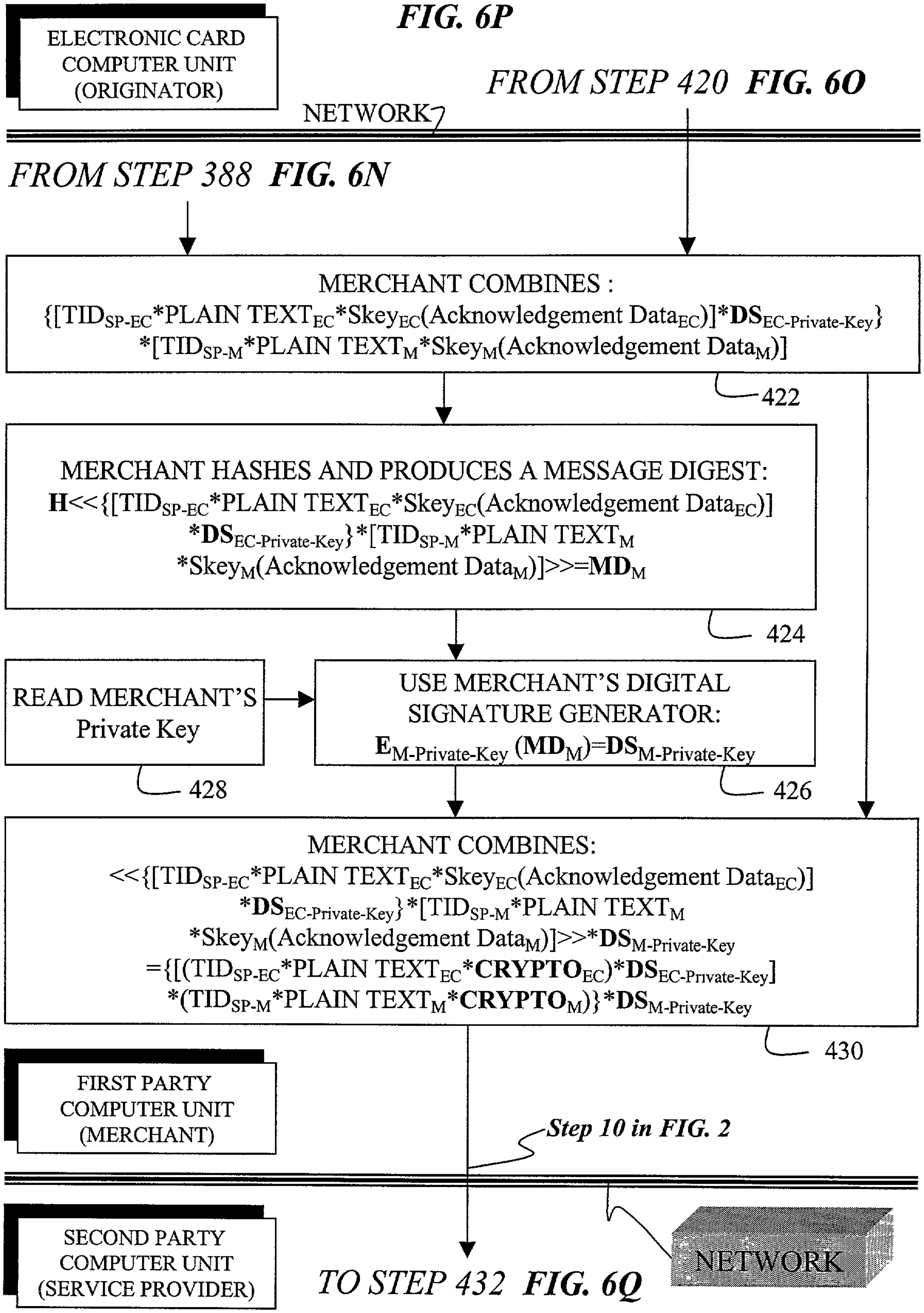

ELECTRONIC CARD COMPUTER UNIT (ORIGINATOR)
FROM STEP 420 FIG. 6O
NETWORK
FROM STEP 388 FIG. 6N
MERCHANT COMBINES :
$\{[TID_{SP\text{-}EC}*PLAIN\ TEXT_{EC}*Skey_{EC}(Acknowledgement\ Data_{EC})]*\mathbf{DS}_{EC\text{-}Private\text{-}Key}\}$
$*[TID_{SP\text{-}M}*PLAIN\ TEXT_{M}*Skey_{M}(Acknowledgement\ Data_{M})]$
422
MERCHANT HASHES AND PRODUCES A MESSAGE DIGEST:
$\mathbf{H}<<\{[TID_{SP\text{-}EC}*PLAIN\ TEXT_{EC}*Skey_{EC}(Acknowledgement\ Data_{EC})]$
$*\mathbf{DS}_{EC\text{-}Private\text{-}Key}\}*[TID_{SP\text{-}M}*PLAIN\ TEXT_{M}$
$*Skey_{M}(Acknowledgement\ Data_{M})]>>=\mathbf{MD}_{M}$
424
READ MERCHANT'S Private Key
428
USE MERCHANT'S DIGITAL SIGNATURE GENERATOR:
$\mathbf{E}_{M\text{-}Private\text{-}Key}\ (\mathbf{MD}_{M})=\mathbf{DS}_{M\text{-}Private\text{-}Key}$
426
MERCHANT COMBINES:
$<<\{[TID_{SP\text{-}EC}*PLAIN\ TEXT_{EC}*Skey_{EC}(Acknowledgement\ Data_{EC})]$
$*\mathbf{DS}_{EC\text{-}Private\text{-}Key}\}*[TID_{SP\text{-}M}*PLAIN\ TEXT_{M}$
$*Skey_{M}(Acknowledgement\ Data_{M})]>>*\mathbf{DS}_{M\text{-}Private\text{-}Key}$
$=\{[(TID_{SP\text{-}EC}*PLAIN\ TEXT_{EC}*\mathbf{CRYPTO}_{EC})*\mathbf{DS}_{EC\text{-}Private\text{-}Key}]$
$*(TID_{SP\text{-}M}*PLAIN\ TEXT_{M}*\mathbf{CRYPTO}_{M})\}*\mathbf{DS}_{M\text{-}Private\text{-}Key}$
430
FIRST PARTY COMPUTER UNIT (MERCHANT)
Step 10 in FIG. 2
SECOND PARTY COMPUTER UNIT (SERVICE PROVIDER)
TO STEP 432 FIG. 6Q
NETWORK

FIG. 6Q

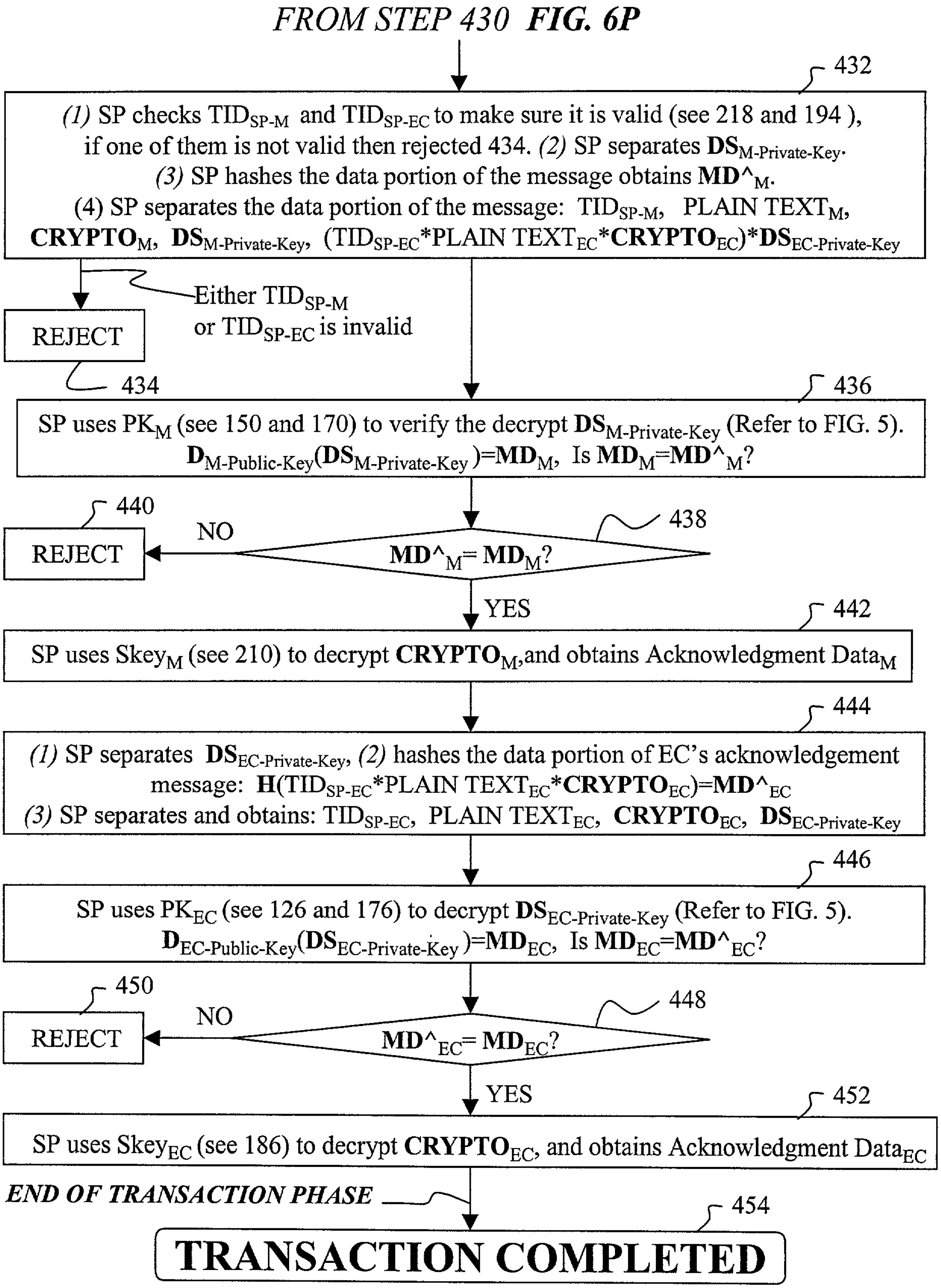

FROM STEP 430 FIG. 6P
432
(1) SP checks TID_{SP-M} and TID_{SP-EC} to make sure it is valid (see 218 and 194), if one of them is not valid then rejected 434. *(2)* SP separates $\mathbf{DS}_{M-Private-Key}$. *(3)* SP hashes the data portion of the message obtains $\mathbf{MD}\hat{}_M$. (4) SP separates the data portion of the message: TID_{SP-M}, PLAIN $TEXT_M$, $\mathbf{CRYPTO}_M$, $\mathbf{DS}_{M-Private-Key}$, ($TID_{SP-EC}$*PLAIN $TEXT_{EC}$*$\mathbf{CRYPTO}_{EC}$)*$\mathbf{DS}_{EC-Private-Key}$
Either TID_{SP-M} or TID_{SP-EC} is invalid
REJECT
434
436
SP uses PK_M (see 150 and 170) to verify the decrypt $\mathbf{DS}_{M-Private-Key}$ (Refer to FIG. 5). $\mathbf{D}_{M-Public-Key}(\mathbf{DS}_{M-Private-Key})=\mathbf{MD}_M$, Is $\mathbf{MD}_M=\mathbf{MD}\hat{}_M$?
440
REJECT
NO
438
$\mathbf{MD}\hat{}_M = \mathbf{MD}_M$?
YES
442
SP uses $Skey_M$ (see 210) to decrypt $\mathbf{CRYPTO}_M$,and obtains Acknowledgment $Data_M$
444
(1) SP separates $\mathbf{DS}_{EC-Private-Key}$, *(2)* hashes the data portion of EC's acknowledgement message: $\mathbf{H}(TID_{SP-EC}$*PLAIN $TEXT_{EC}$*$\mathbf{CRYPTO}_{EC})=\mathbf{MD}\hat{}_{EC}$ *(3)* SP separates and obtains: TID_{SP-EC}, PLAIN $TEXT_{EC}$, $\mathbf{CRYPTO}_{EC}$, $\mathbf{DS}_{EC-Private-Key}$
446
SP uses PK_{EC} (see 126 and 176) to decrypt $\mathbf{DS}_{EC-Private-Key}$ (Refer to FIG. 5). $\mathbf{D}_{EC-Public-Key}(\mathbf{DS}_{EC-Private-Key})=\mathbf{MD}_{EC}$, Is $\mathbf{MD}_{EC}=\mathbf{MD}\hat{}_{EC}$?
450
REJECT
NO
448
$\mathbf{MD}\hat{}_{EC} = \mathbf{MD}_{EC}$?
YES
452
SP uses $Skey_{EC}$ (see 186) to decrypt $\mathbf{CRYPTO}_{EC}$, and obtains Acknowledgment $Data_{EC}$
END OF TRANSACTION PHASE
454
TRANSACTION COMPLETED

FIG.7

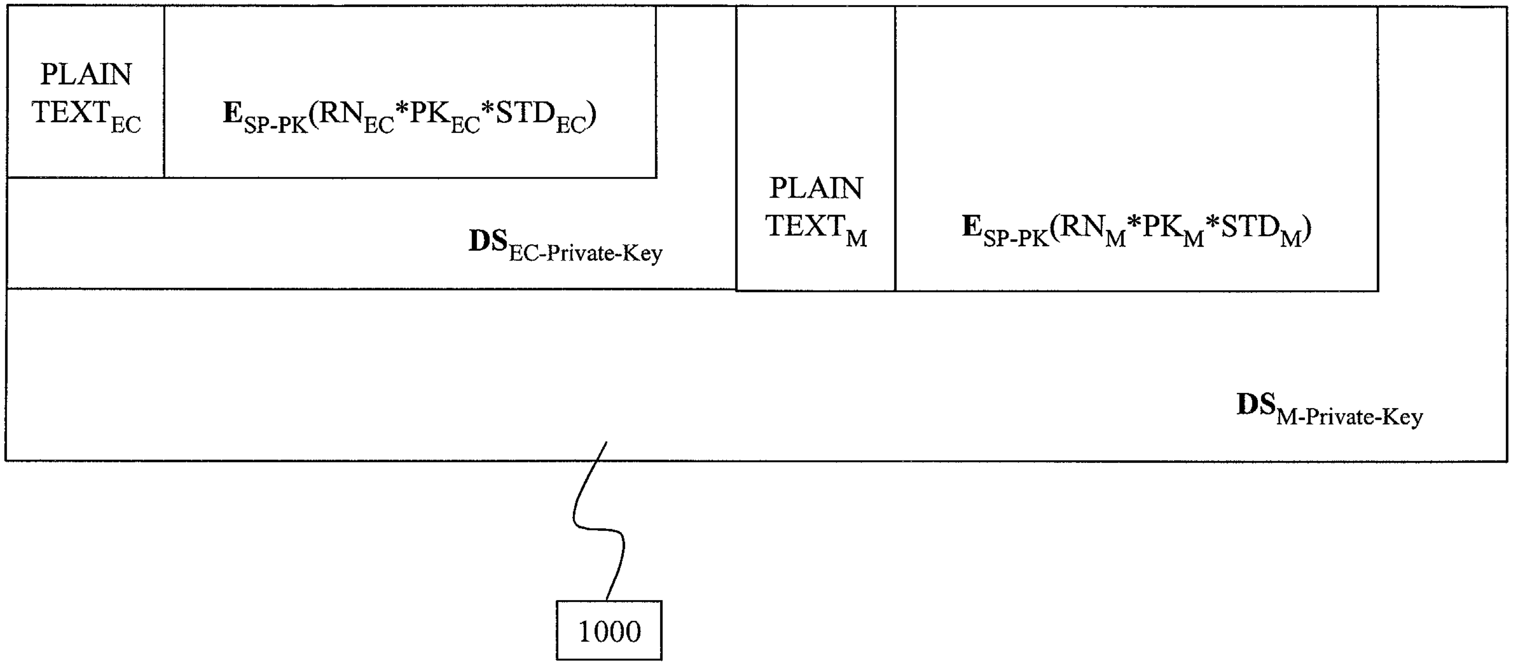

PLAIN TEXT$_{EC}$
$\mathbf{E}_{SP\text{-}PK}(RN_{EC}*PK_{EC}*STD_{EC})$
$\mathbf{DS}_{EC\text{-}Private\text{-}Key}$
PLAIN TEXT$_{M}$
$\mathbf{E}_{SP\text{-}PK}(RN_{M}*PK_{M}*STD_{M})$
$\mathbf{DS}_{M\text{-}Private\text{-}Key}$
1000

FIG.8

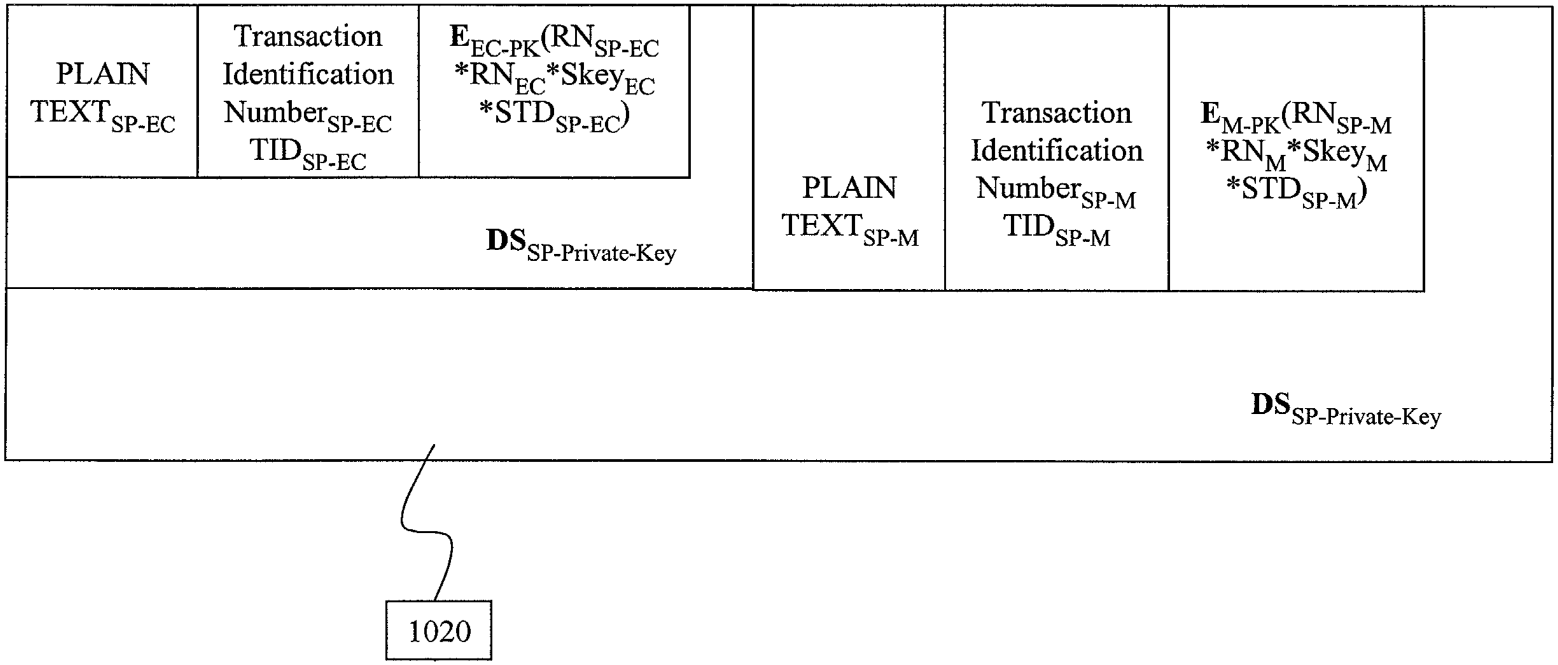

PLAIN TEXT$_{SP-EC}$
Transaction Identification Number$_{SP-EC}$ TID$_{SP-EC}$
$\mathbf{E}_{EC\text{-}PK}(RN_{SP\text{-}EC} * RN_{EC} * Skey_{EC} * STD_{SP\text{-}EC})$
$\mathbf{DS}_{SP\text{-}Private\text{-}Key}$
PLAIN TEXT$_{SP-M}$
Transaction Identification Number$_{SP-M}$ TID$_{SP-M}$
$\mathbf{E}_{M\text{-}PK}(RN_{SP\text{-}M} * RN_{M} * Skey_{M} * STD_{SP\text{-}M})$
$\mathbf{DS}_{SP\text{-}Private\text{-}Key}$
1020

FIG.9

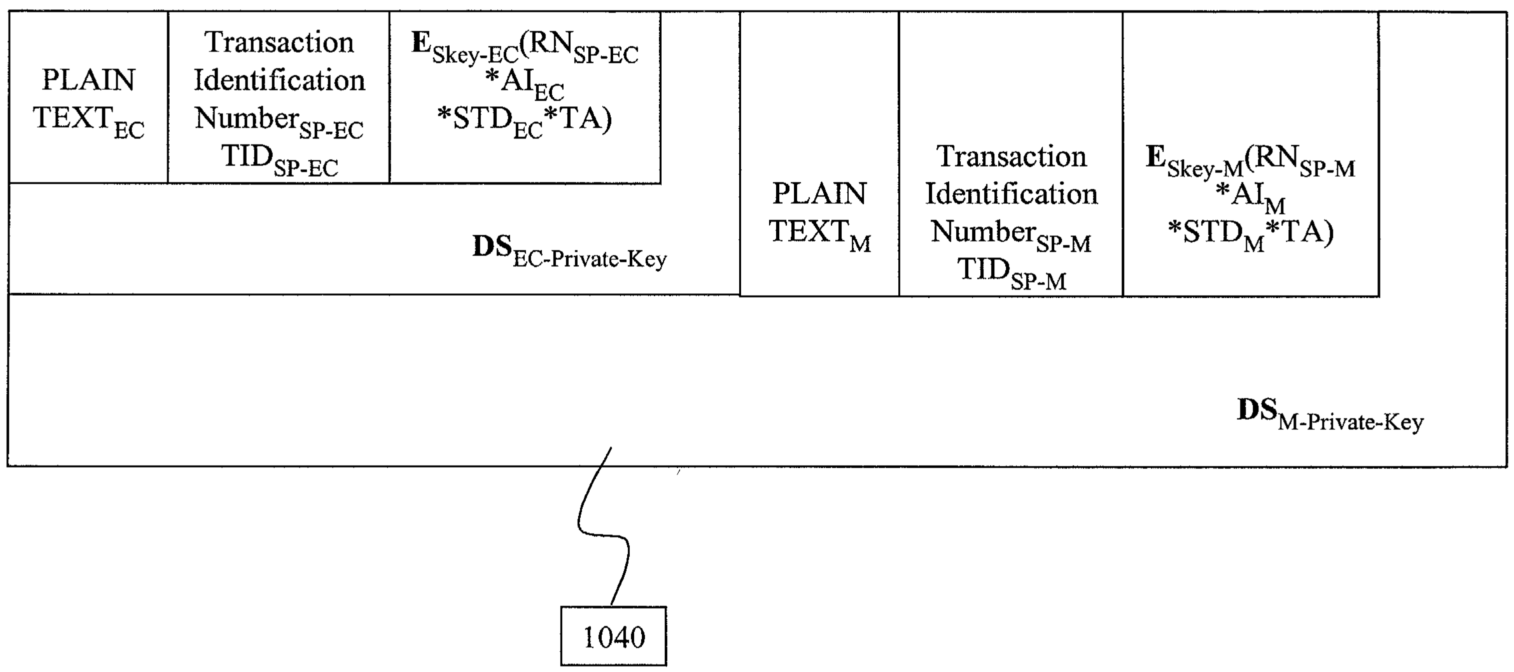

PLAIN TEXT$_{EC}$
Transaction Identification Number$_{SP-EC}$ TID$_{SP-EC}$
E$_{Skey-EC}$(RN$_{SP-EC}$ *AI$_{EC}$ *STD$_{EC}$*TA)
DS$_{EC-Private-Key}$
PLAIN TEXT$_M$
Transaction Identification Number$_{SP-M}$ TID$_{SP-M}$
E$_{Skey-M}$(RN$_{SP-M}$ *AI$_M$ *STD$_M$*TA)
DS$_{M-Private-Key}$
1040

FIG.10

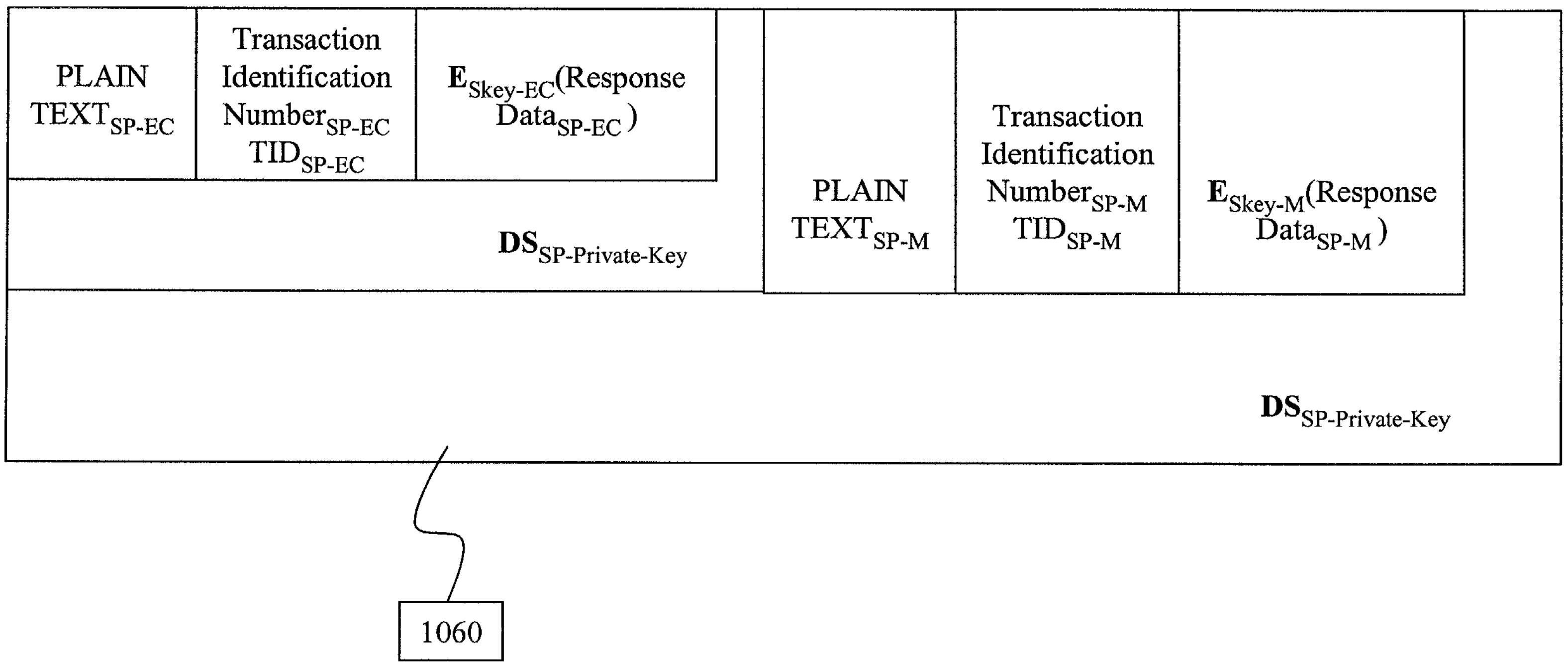

PLAIN TEXT$_{SP-EC}$
Transaction Identification Number$_{SP-EC}$ TID$_{SP-EC}$
$\mathbf{E}_{Skey-EC}$(Response Data$_{SP-EC}$)
$\mathbf{DS}_{SP-Private-Key}$
PLAIN TEXT$_{SP-M}$
Transaction Identification Number$_{SP-M}$ TID$_{SP-M}$
$\mathbf{E}_{Skey-M}$(Response Data$_{SP-M}$)
$\mathbf{DS}_{SP-Private-Key}$
1060

FIG.11

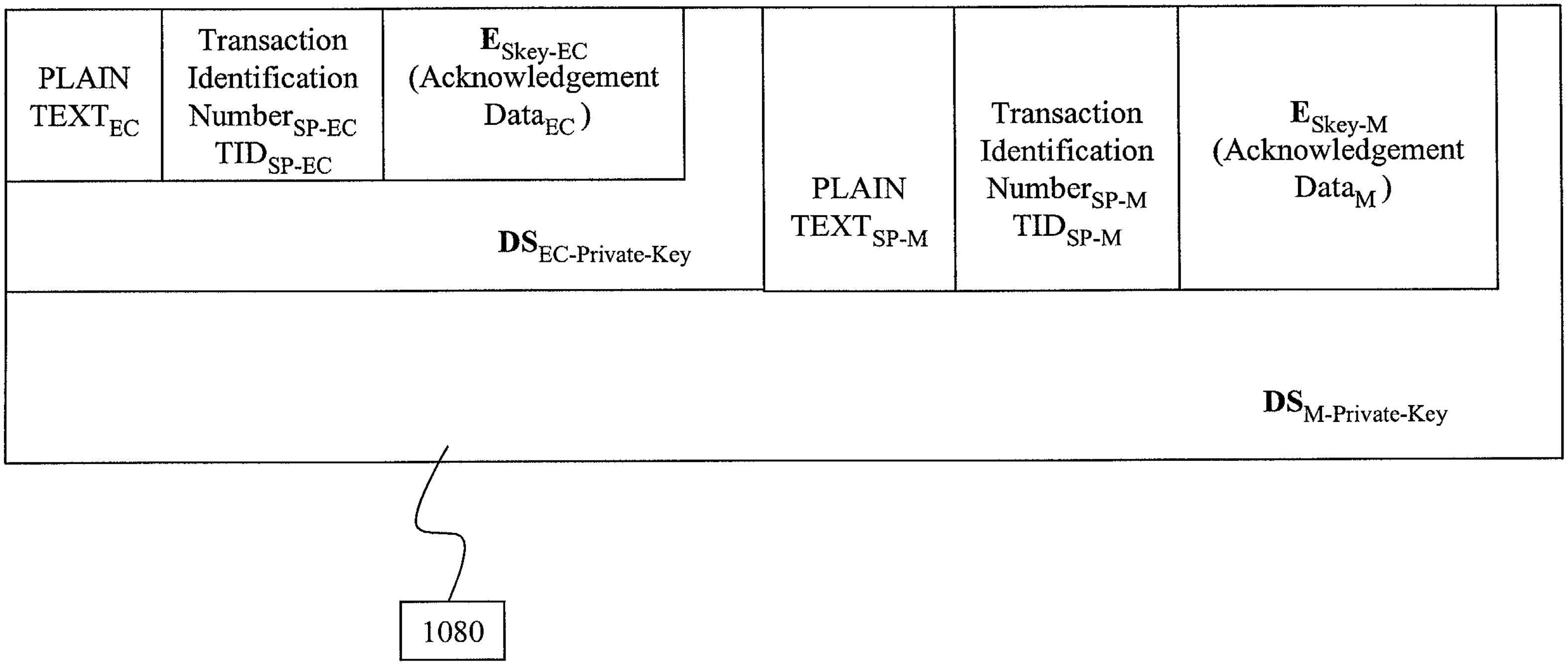

PLAIN TEXT$_{EC}$
Transaction Identification Number$_{SP-EC}$ TID$_{SP-EC}$
E$_{Skey-EC}$ (Acknowledgement Data$_{EC}$)
DS$_{EC-Private-Key}$
PLAIN TEXT$_{SP-M}$
Transaction Identification Number$_{SP-M}$ TID$_{SP-M}$
E$_{Skey-M}$ (Acknowledgement Data$_{M}$)
DS$_{M-Private-Key}$
1080

FIG. 12

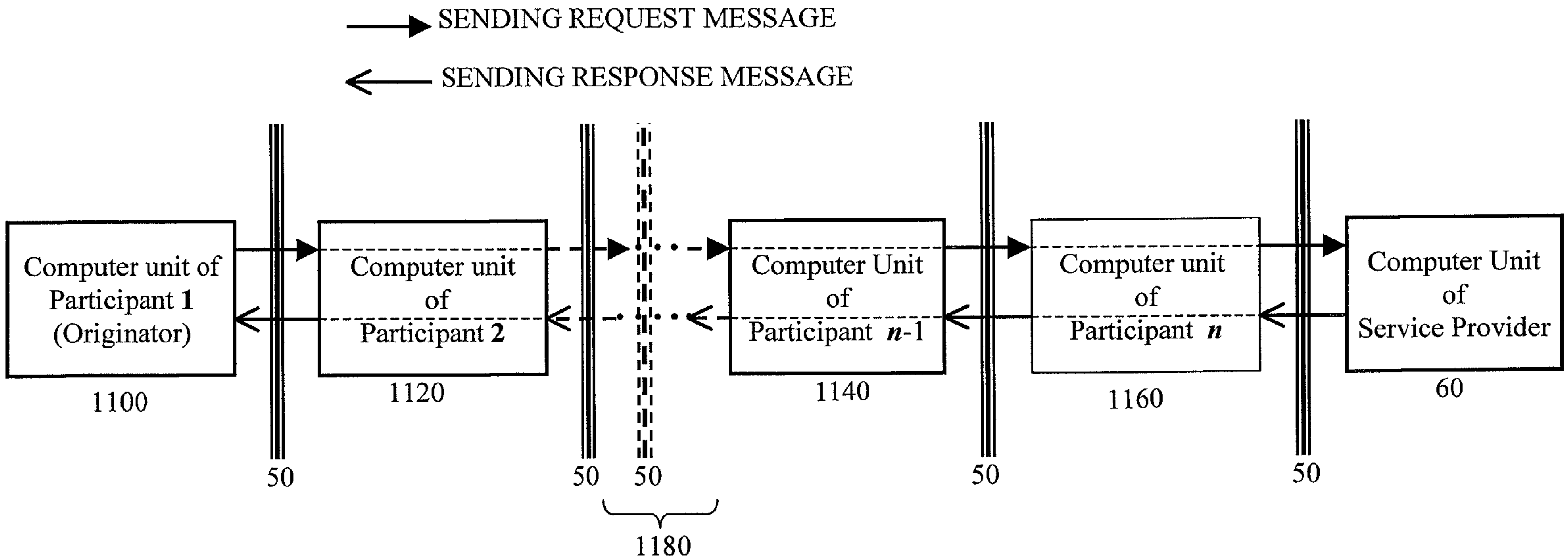
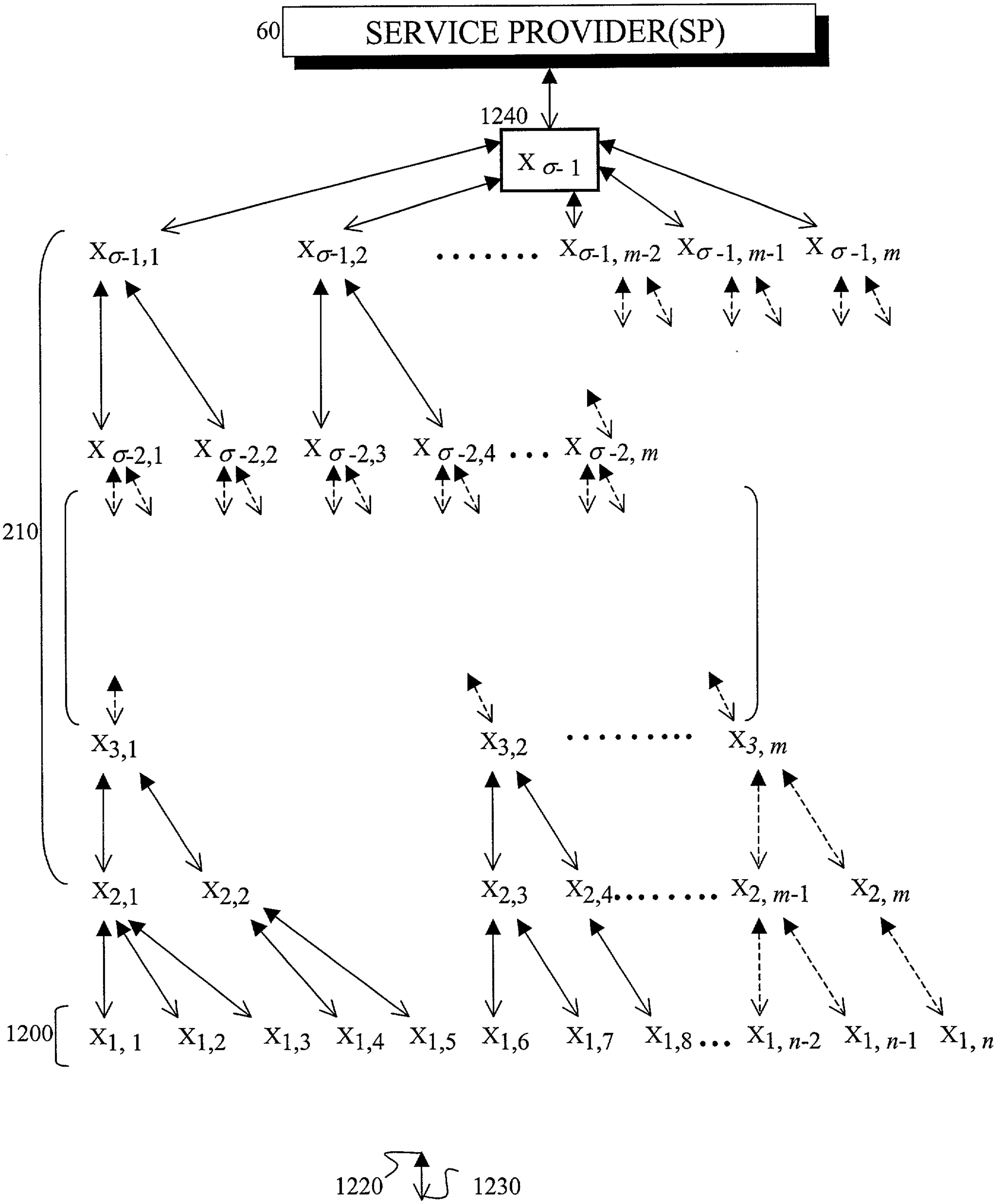

SENDING REQUEST MESSAGE
SENDING RESPONSE MESSAGE
Computer unit of Participant 1 (Originator)
1100
Computer unit of Participant 2
1120
Computer Unit of Participant n-1
1140
Computer unit of Participant n
1160
Computer Unit of Service Provider
60
50
50
50
50
50
1180

FIG. 13



60
SERVICE PROVIDER(SP)
1240
$X_{\sigma\text{-}1}$
$X_{\sigma\text{-}1,1}$
$X_{\sigma\text{-}1,2}$
....
$X_{\sigma\text{-}1,m\text{-}2}$
$X_{\sigma\text{-}1,m\text{-}1}$
$X_{\sigma\text{-}1,m}$
$X_{\sigma\text{-}2,1}$
$X_{\sigma\text{-}2,2}$
$X_{\sigma\text{-}2,3}$
$X_{\sigma\text{-}2,4}$
...
$X_{\sigma\text{-}2,m}$
1210
$X_{3,1}$
$X_{3,2}$
....
$X_{3,m}$
$X_{2,1}$
$X_{2,2}$
$X_{2,3}$
$X_{2,4}$........
$X_{2,m\text{-}1}$
$X_{2,m}$
1200
$X_{1,1}$
$X_{1,2}$
$X_{1,3}$
$X_{1,4}$
$X_{1,5}$
$X_{1,6}$
$X_{1,7}$
$X_{1,8}$...
$X_{1,n\text{-}2}$
$X_{1,n\text{-}1}$
$X_{1,n}$
1220
1230

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATIONS

PATENT

Docket No. : 34581/AH/C718

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled A CRYPTOGRAPHIC SYSTEM AND METHOD FOR ELECTRONIC TRANSACTIONS, the specification of which is attached hereto unless the following is checked:

__ was filed on __ as United States Application Number or PCT International Application Number __ and was amended on ___ (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR § 1.56.

I hereby claim foreign priority benefits under 35 U.S.C. § 119(a)-(d) or § 365(b) of the foreign application(s) for patent or inventor's certificate, or § 365(a) of any PCT International application which designated at least one country other than the United States, listed below and have also identified below, any foreign application for patent or inventor's certificate, or PCT International application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application(s)

Application Number	Country	Filing Date (day/month/year)	Priority Claimed
PCT/US99/09938		05/05/99	YES

I hereby claim the benefit under 35 U.S.C. § 119(e) of any United States provisional application(s) listed below.

Application Number	Filing Date
60/084,257	05/05/98

I hereby claim the benefit under 35 U.S.C. § 120 of any United States application(s), or any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of 35 U.S.C. § 112, I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR § 1.56 which became available between the filing date of the prior application and the national or PCT International filing date of this application:

Application Number	Filing Date	Patented/Pending/Abandoned

POWER OF ATTORNEY: I hereby appoint the following attorneys and agents of the law firm CHRISTIE, PARKER & HALE, LLP to prosecute this application and any international application under the Patent Cooperation Treaty based on it and to transact all business in the U.S. Patent and Trademark Office connected with either of them in accordance with instructions from the assignee of the entire interest in this application;

or from the first or sole inventor named below in the event the application is not assigned; or from __ in the event the power granted herein is for an application filed on behalf of a foreign attorney or agent.

R. W. Johnston	(17,968)	John D. Carpenter	(34,133)	Lucinda G. Auciello	(42,270)
D. Bruce Prout	(20,958)	David A. Plumley	(37,208)	Norman E. Carte	(30,455)
Hayden A. Carney	(22,653)	Wesley W. Monroe	(39,778)	Joel A. Kauth	(41,886)
Richard J. Ward, Jr.	(24,187)	John W. Eldredge	(37,613)	Patrick Y. Ikehara	(42,681)
Russell R. Palmer, Jr.	(22,994)	Gregory S. Lampert	(35,581)	Mark Garscia	(31,953)
LeRoy T. Rahn	(20,356)	Grant T. Langton	(39,739)	Gary J. Nelson	(44,257)
Richard D. Seibel	(22,134)	Constantine Marantidis	(39,759)	Raymond R. Tabandeh	(43,945)
Walter G. Maxwell	(25,355)	Daniel R. Kimbell	(34,849)	Phuong-Quan Hoang	(41,839)
William P. Christie	(29,371)	Craig A. Gelfound	(41,032)	Jun-Young E. Jeon	(43,693)
David A. Dillard	(30,831)	Syed A. Hasan	(41,057)	Kathy Mojibi	(41,409)
Thomas J. Daly	(32,213)	Kathleen M. Olster	(42,052)	Cynthia A. Bonner	(44,548)
Vincent G. Gioia	(19,959)	Daniel M. Cavanagh	(41,661)	Marc A. Karish	(44,816)
Edward R. Schwartz	(31,135)	Molly A. Holman	(40,022)		

The authority under this Power of Attorney of each person named above shall automatically terminate and be revoked upon such person ceasing to be a member or associate of or of counsel to that law firm.

DIRECT TELEPHONE CALLS TO : **Craig A. Gelfound, 626/795-9900**
SEND CORRESPONDENCE TO : **CHRISTIE, PARKER & HALE, LLP**
P.O. Box 7068, Pasadena, CA 91109-7068

I declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full name of sole or first joint inventor Jay C. Chen	Inventor's signature	Date
Residence and Post Office Address 1355 Blackstone Road, San Marino, California 91108		Citizenship United States

CMM PAS221074.1-*-12/8/99 10:48 AM